ISSUE 3SUMMER TERM

2005

NEWSLETTER



Institute for Quantum Computing

On Monday May 1st, 2005, the University of Waterloo announced receipt of a "magnificent" gift from Ophelia and Mike Lazaridis.

Ophelia and Mike Lazaridis have personally donated \$17.2 million in addition to last year's \$33.3 million gift for the Institute for Quantum Computing.



Photo from UW Daily Bulletin

The additional gift will fund three exciting and related initiatives: 75 per cent towards a shared new facility housing the university's Institute for Quantum Computing and Nanotechnology Engineering Program and the remaining 25 per cent towards an endowment to attract the very best foreign graduate students involved in quantum studies. Each student will receive a \$20,000 scholarship from the endowment, and a President's Graduate Scholarship equivalent to full tuition, currently valued at \$13,770.

Mike Lazaridis is the University's Chancellor and the founder, president and Co-CEO of Research In Motion. In April, he was listed as one of this year's "100 most influential people" by *Time* magazine.

"The University of Waterloo is once again blessed by our chancellor's outstanding commitment to our university's mission," said UW President David Johnston. "This is a magnificent gift to the university and will be used for developing outstanding national programs, researchers and grad students in quantum computing and nanotechnology engineering."

Lazaridis said: "Ophelia and I are grateful to be in a position to contribute and we are proud to see this important research happening within our community and country. We believe accelerated research and education in Quantum Computing and Nanotechnology Engineering will change the technological landscape and benefit mankind for generations to come."

Plans for a new facility to house Nanotechnology Engineering and Quantum Computing research and teaching are already well underway. The new building will be situated in the centre of the university's campus. (Details in *Media* section)

Attracting students of the highest quality to quantum research gives tremendous support to creativity and research, while also enhancing the capacity of the Canadian economy through the infusion of talent, new discoveries and potential commercial spin-offs.



BFG Building

| In This Issue | |
|------------------|----|
| Recent Events | 2 |
| ▶ Graduates | 4 |
| Recognition | 5 |
| ▶ IQC's New Lab | 6 |
| ► Joining Us | 7 |
| People on the Go | 8 |
| ▶ Media | 10 |
| Visitors | 11 |
| Thanks | 12 |



200 University Ave. West, Waterloo, ON, N2L 3G1, Canada *phone* (519) 888-4021 *fax* (519) 888-7610 www.iqc.ca



RECENT EVENTS

Anton Zeilinger, University of Vienna

Professor Anton Zeilinger, a prominent scientist, visited Waterloo's quantum physics community in early March. On Wednesday March 2nd, Zeilinger gave a talk at Waterloo Collegiate Institute entitled, "From Einstein to Quantum Information." On March 3rd, Zeilinger spoke at IQC on "Interpretation of Quantum Mechanics."

Attendees of his talks were privileged to listen to the world-renowned physicist who has held teaching and research positions at:

- M.I.T.
- -University of Innsbruck
- University of Oxford
- Vienna Technical University
- Munich Technical University
- College de France in Paris

Currently, he is a professor of Physics at the University of Vienna.



Robert J. Sawyer

Anton Zeilinger is also known as 'Mr. Beam' for his most recognized work: In 1997, Zeilinger and his colleagues confirmed aspects of quantum teleportation by actually teleporting light particles. Recently, Zeilinger and his colleagues were the first to demonstrate quantum interference on the biggest system so far: the Buckyball, a soccer ball shaped macromolecule made of 60 carbon atoms.

Visit Professor Zeilinger's home page: http://www.quantum.univie.ac.at/zeilinger/

Colm Ryan talks at One Book, One Community Event

The Canadian writer, Robert J. Sawyer, participated in the annual One Book, One Community event held in IQC's seminar room on the morning of Saturday June 11th, 2005. This literary event promotes one novel each year within the tri-city area by urging people to engage in reading and talking about the same book. This year's selection is Robert Sawyer's anthropological science



fiction novel, "Hominids"; which precedes "Humans" and "Hybrids" in a trilogy. "Hominids", the 2003 Hugo Best Novel Award winner, is a well researched piece of writing that absorbs us into the results of a quantum computing experiment, causing a Neanderthal to be transported into our present world. Throughout the day, people on a bus tour listened to talks discussing the themes in "Hominids". Colm Ryan represented IQC as he spoke about quantum computing, a major theme in the book. Colm introduced some basic ideas about quantum mechanics and quantum computing and possible applications for quantum computing. The audience was thrilled to be exposed to the world of quantum mechanics.

Weekly Quantum Cryptography and **Optics Discussion**

Since February 2005, IQC and faculty students members have been meeting for a weekly quantum cryptography and optics discussion group. Each week, this group meets for informal talks and discussions on theoretical and practical topics in quantum cryptography.

One of the aims of the group is to bring people from different disciplines together. The group has included theoretical and experimental physicists, mathematicians, computer scientists, and engineers. Previous topics have included the Shor and Preskill proof of security of quantum key distribution, decoy state QKD, quantum fingerprinting, QKD in the context of superluminal signaling, and components of cryptographic systems, such as optical hardware, repeaters, and hash functions.

Our discussions are linked via video conferencing with the Institute for Quantum Information Science at the University of Calgary.

For more information about the discussion group, contact Lana Sheridan (lssherid@iqc.ca) or Douglas Stebila (dstebila@iqc.ca).







Institute for Quantum Computing

Site Visit

Over 60 participants contributed to the site visit, including researchers from universities across Canada, industry and government partners, graduate students, postdocs, senior University of Waterloo management and IQC staff. Sessions included a network overview by Ray Laflamme, and presentations by theme leaders Richard Cleve from IQC, who reviewed the Quantum Algorithms and Complexity theme, Barry Sanders, from the University of Calgary, who discussed the Quantum Building Blocks theme and Michele Mosca from IQC spoke for Gilles Brassard (from the University of Montreal who was not able to attend the site visit) on Quantum Cryptography theme.

Representatives from industry and government laboratory partners including Research in Motion, Sun Microsystems, General Dynamics Canada, Bruker Biospin, the National Research Council, Nortel and the Perimeter Institute participated in a discuss of the value and benefits of QuantumWorks to the Canadian industry.

Thanks to the enthusiastic participation of all involved, the site visit was a resounding success and an impressive complement to the QuantumWorks funding proposal submitted to NSERC in February. News on funding for QuantumWorks is expected in June and will be reported in the next IQC newsletter.

Coherent Spintronics Workshop

On May 16th and 17th, IQC hosted a two-day mini-conference with David Cory's MIT research group. The workshop was titled "Coherent Spintronics" and focused on developments in new and existing technologies for the coherent control of quantum systems--a major hurdle to be overcome before practical quantum computers can be built. Topics presented included heat bath algorithmic cooling, superconducting flux qubits, quantum error models, and recent innovations in nanotechnology. About 20 representatives from various affiliations which included IQC, The Perimeter Institute, MIT's Department of Nuclear Science & Engineering and the MIT Lincoln Laboratory, participated in the workshop. This conference marks a growing collaborative effort between IQC and our colleagues at MIT, and we look forward to similar events in the near future.



GRADUATES

A Quantum Algorithm for Finding An ϵ -Approximate Mode



Aziz Kara I have really enjoyed my time at IQC and am really thankful to all those who have made this possible. I also thank all those who selflessly lent their help and support.

Institute for Quantum Computing

Consider a list S of size N whose elements are drawn from a set D of size M. The statistical mode of S is the number that occurs most often in S. For example, if D = {1,2,3} and S={1,2,3,1,3,2,3,2,1,2,2}, then the mode of S is 2 as it occurs most often, five times. We define an ϵ -approximate mode of S as any element whose frequency in the list is within ratio (1+ ϵ), ϵ > 0, of the frequency of the modal element.

The main result in my thesis is the development of a quantum algorithm for finding an ϵ -approximate mode. More specifically, with probability at least 1- δ , δ >0, the algorithm finds an element of the list whose estimated frequency is within ratio (1+ ϵ) of the frequency of the modal element. It uses a number of list queries that is a polynomial in M, 1/ ϵ and log(1/ δ) to find an ϵ -approximate mode.

A key ingredient of the algorithm is a uniformized quantum phase

estimation algorithm. Standard quantum phase estimation approximates the value of a phase parameter in the phase of an eigenvector of a given unitary operator. An important application of quantum phase estimation is counting: given a problem instance x, one can use phase estimation to approximate the number of solutions to x. This information is encoded in the phase of an eigenvector of a suitable Grover iterate. As it turns out, the quality of the estimate is directly dependent on the value of the phase parameter, itself. This poses problems if one wishes to use these estimates within a quantum algorithm. Informally, uniformization attempts to remove this dependency to a large degree by dampening this direct dependence. Uniformized phase estimation is discussed at length in my thesis with a look at how this dependence is dampened.

The last section of the thesis explores an application of the approximate mode finding procedure in quantizing an approximate counting scheme of Jerrum, Valliant and Vazirani. Their scheme makes use of an almost-uniform generator for combinatorial objects which is repeatedly queried in order to gather certain statistics. In addition to the generator, they make use of a classical mode finding scheme which we replace with the quantum approximate mode finding procedure to illustrate an almost quadratic speed-up in the approximate counting scheme.

On Heat-Bath Algorithmic Cooling and Its implementation in Solid-State NMR

Motivation: Preparation of a quantum computer in a known state is essential for quantum computation. This is required in initializing a quantum computer for computation, and in dynamically supplying ancilla qubits to achieve fault-tolerance. Heat-bath algorithmic cooling is an implementation-independent procedure, which has been proposed as means to purify the initially mixed state for computation.

The **contribution** of the thesis, as implied by its title, is two fold:

Theoretical: Numerical simulations of the heat-bath algorithmic cooling procedure, highlighting the theoretical limits on achievable cooling using this algorithm.

Experimental: Reporting the implementation of this algorithm on a 3qubit processor as a proof of principle. The experiment is performed using the nuclear magnetic resonance (NMR) of single-crystal Malonic Acid (C3H4O4) in the solid state. Using the algorithm, and starting from the totally mixed state on the computational qubits, we are able to cool one of the qubits below the effective heat-bath temperature.



Osama Moussa

I would like to thank everyone at the IQC, <u>who have m</u>ade my experience a rich and pleasant one. In particular: Raymond, Jonathan, Marcus, Colm, Ashwin, and Wendy. This was also supported by the Ontario Graduate Scholarship Program.

Tim Reid completed his Masters in math in the Combinatorics and Optimization department. His thesis was entitled "On the Evolutionary Design of Quantum Circuits."





Laval University Pays Tribute to Ray Laflamme

On May 13th 2005, **Ray Laflamme** received the *Gloire de l'Escolle* medal during the *Grands Diplomes* award ceremony at the Laval University in Quebec City. The president of the University alumni association, Dominique Houde, presented the award with Mr. Michel Pigeon, the University President. Ray was one of eight graduates honoured with the medal. Each year, the medal recognizes the exceptional merit of some of Laval's graduates who brilliantly conducted their career and who constitute as role models for students and a source of pride for all Laval University graduates.

Photo: (left to right) Dominique Houde, Ray Laflamme, Michel Pigeon

- Martin Laforest received the Doctorate Scholarship from the FQRNT (Fond Québécois de la Recherche sur la Nature et les Technologies) for 3 years and was ranked 4th out of 45 applicants by the physics and astrophysics committee.
- **Dr. A. Hamed Majedi** received a tenure track position as Assistant Professor in the Electrical and Computer Engineering Department.
- Dr. Gregor Weihs was awarded the NSERC Discovery Grant, entiltled, "Tools for photonics quantum entanglement". Starting April 1st, 2005, Dr. Weihs' research group will receive \$43,500 a year for 5 years.
- David Poulin was awarded the W.B. Pearson Medal in the Faculty of Science for recognition of creative research as presented in his Ph.D. thesis.

NSERC Awards

NSERC (The Natural Sciences and Engineering Research Council of Canada), the primary federal agency funding university research and training in natural sciences and engineering, invests in people, discovery and innovation. NSERC supports university students and postdoctoral fellows completing advanced studies with **CGS** (Canada Graduate Scholarship), **PGS** (Postgraduate Scholarship) and **USRA** (Undergraduate Student Research Award) awards.

The CGS and PGS awards promote research careers in natural sciences and engineering. The CGS and PGS are awarded to excellent full-time students enrolled in a masters or doctoral program who have obtained an average of at least "A-" in both of their previous two years of studies completed.

The USRA award encourages students to continue their studies in their fields by beginning graduate studies.



Nathan Babcock USRA Award Recipient



JC. Boileau PGS Award Recipient



Martin Laforest PGS Award Recipient



Paul McGrath USRA Award Recipient



Colm Ryan CGS Award Recipient



Marcus D. Silva PGS Award Recipient



Dr. Gregor Weihs' Photonic Entanglement Lab

newly formed Photonic The Entanglement Group under the direction of Prof. Gregor Weihs has just started the development of their new Photonic Entanglement Laboratory located in the BFG building. With the old server equipment on its way to an adjacent room, lab desks and one optical table have already made their way into the lab. A second, much larger, optical table is arriving in June to complete the lab. The smaller optical table currently in the lab will be housing a Quantum Key Distribution (QKD) experiment while the larger table is set to hold research on novel sources of entangled photon pairs based on semiconductor nanostructures.

Institute for Quantum Computing

The QKD experiment will implement a free-space optical link between source, producing entangled а photon pairs, and two receivers, which will use the entangled photons to build-up a secure key. As shown in the picture to the right, the source will be located on either the Physics building or the Davis Centre library according to line-ofsite requirements and the two receivers will be placed at the Perimeter Institute and the Institute for Quantum Computing. The experiment will also allow the study of the proper error model for a freespace link.

While the basic protocols of quantum key distribution have been

proven to be secure, there are a great number of cryptographic tasks that have no (known) quantum solution and thus need the help of classical cryptography. The QKD experiment is meant to bring physicists from IQC together with cryptographers from the Centre for Applied Cryptographic Research at the University of Waterloo to analyze some of the cryptographic tasks. Additionally, having a working quantum key distribution



system will allow the testing of new protocols that have not been implemented before along with some of the outstanding security issues in QKD. These tests will possibly include: multi-pair emission security issues, multi-state protocols, multi-photon protocols, fundamental tests, and quantum fingerprinting.

Some quantum computing implementations and certain metrology applications require entangled photon pairs as essential resource, not only for quantum key distribution but also for a variety of other quantum communication protocols. Currently, they are typically produced by very inefficient nonlinear optical processes in bulk crystals. Their production suffers from the dispersion in natural materials and also from the fact that in the nonlinear optic production sometimes more that one photon pair is produced at a time. Ideally, we would like to have an efficient source that produces a single pair each time we "push a button". Quantum dots, nanoscopic semiconductor structures that confine charge carriers could serve as photon pair sources.

Another route is to engineer the dispersion to fit the needs of the nonlinear optical process. Photonic crystals, periodic structures in optical materials, provide a way of creating optical microscopic optical circuits. They can also enable or enhance the optical nonlinearity of a material that would otherwise be useless for the production of photon pairs. Both quantum dots and photonic crystal waveguides will be investigated in the new laboratory that will house an ultrafast laser system, a high resolution spectrometer, cryostats and high-speed photon counting instrumentation.





JOINING US

Welcome



Nathan Babcock completed his B.Sc. in Honours Physics at the University of Waterloo. Though his research career began in soft materials and complex fluids, he's since developed a deep interest in guantum information. After working at IQC for the summer, he will be doing his graduate work at the Institute for Quantum Information Science in Calgary, Alberta.

Chris Erven completed his BASc in Honours Co-op Systems Design Engineering with a physics option at the University of Waterloo. Chris is starting his Masters in Quantum Computing under the co-supervision of Ray Laflamme and Gregor Weihs. Chris plans to continue his PhD in the areas of quantum foundations, string theory, and M Theory.





Rolf Horn has a B.Eng and a MSc., both obtained in physics at the Queen's University, Kingston. He worked as a research assistant in the field of low temperature physics and then in quantum information science with Dr. Barry Sanders at the Institute for Quantum Information Science at the University of Calgary. He now works with Gregor Weihs.

Paul McGrath is an undergraduate student at the University of Waterloo, majoring in the Mathematical Physics program. He will be working with Ray Laflamme and Gregor Weihs to conduct research in quantum cryptography. Paul plans to continue studying quantum computing at the graduate level.





A little Emerson

Joseph Emerson, an IQC affiliate member, and his wife Kate, became the proud parents of Anabelle Elizabeth Emerson on Tuesday, April 19th, 2005.

Congratulations to Joseph and his family!

SUMMER STUDENTS



William Donnelley **Research Assistant**

LONG TERM VISITORS



Arvid Bessen Columbia University June 1-August 31



Dushy Kent Co-op Student

Mika Hirvensalo

University of Turku, Finland

June 6-November 1



Kelly J. Rose **Research Assistant**



IQC is pleased to welcome Adele Newton. She joined IQC in January as our Director of Industry and Government Relations.





Iordanis Kerenidis MIT June 1-30



Ben Reinhardt Berkelev June 6-July 15

PEOPLE ON THE GO



Institute for Quantum Computing

Dr. Gregor Weihs spoke at the American Physical Society meeting, held March 21st-25th in Los Angeles. He was also invited to talk at the 9th International Conference on Squeezed States and Uncertainty Relations (ICSSUR), held May 2nd-6th in Besancon, France. As a member of the Organizing Team for the Quantum Physics of Nature (QUPON), Dr. Weihs was one of 300 quantum physicists to attend the Quantum Physics of Nature & 6th European QIPC Workshop., in Vienna.



Jamie Batuwantudawe also attended the Quantum Physics of Nature & 6th European QIPC Workshop in Vienna. On May 22nd, Jamie presented a poster entitled "A Look at a Three State Quantum Key Distribution Protocol". Earlier, Jamie visited the group of Nicolas Gisin at Geneva University and the group of Norbert Luetkenhaus at the University of Erlangen-Nurnberg. On May 27th, 2005, he attended the SECOQC 2nd General Assembly in Vienna, Austria.



The Great Hall: QUPON conference talk in The University of Vienna's main building.



Christoph Dankert visited Mario Szegedy from March 20th-26th at Rutgers, The State University of New Jersey. Together with two of Szegedy's graduate students, Christoph looked into the differences between continuous time and discrete time quantum random walks.

On March 26th, he attended the Theory & Lunch talk hosted by the Computer Science Department at Princeton University. Subhash Khot from Georgia Tech., gave the talk, "On embeddability of negative type metrics into I_1". In the afternoon, Christoph discussed various issues in Theoretical Computer Science with Mario Szegedy and Noga Alon at the Institute for Advanced Study.



Marcus D. Silva visited the IBM Thomas J. Watson Research Center at Yorktown Heights, New York, from February 28th to March 4th. He started a collaboration with Barbara Terhal and David DiVicenzo on the calculation of error thresholds for fault tolerant quantum computation.



Thomas J. Watson Research Center

MOVING ON



Dr. Pranab Sen joined NEC Labs, Princeton in April 2005 as a Research Staff Member, working in the Quantum Information Technology group. Pranab works with Martin Roetteler (a former IQC member) and Sean Hallgren. Pranab will be continuing his research in quantum algorithms, quantum communication complexity and privacy issues in quantum communication and key distribution.

Congratulations to Pranab and good luck with your future endeavours

Page 8 of 12

PEOPLE ON THE GO

Elham Around the World

Finally, May 10th-15th, Elham attended the RESQ Workshop in **Budapest** to present recent research taking place at the University of Waterloo. On Friday May 13th, Elham gave a talk on Information flow for graph states entitled "Measurement based quantum computing".

Institute for Quantum Computing



Elham Kashefi was invited by Professor Hans Briegel to visit his quantum information group at the University of Innsbruck, *Austria* from February, 7th -12th. Elham collaborated with Briegel on her recently published work on one-way model:

> publication listed: www.iqc.ca/publications/

Elham also attended the Causality, Spacetime Topology Domain Theory workshop held April 24th -29th at the Bellairs Research Institute in **Barbados**. The Bellairs Research Institute of McGill University is Canada's only teaching and research facility in the Caribbean.





After being invited by Professor Vincent Danos to visit the PPS (PREUVES, PROGRAMMES et SYSTÈMES) lab at the University of Paris, Elham spent a few days in *France*; April 11th-16th, completing several projects on measurement based quantum computing with Danos.

During her visit to the PPS lab, Elham also spoke at the PPS seminar on Thursday April 14th about programming quantum computing. Her talk was entitled "The measurement calculus".

University of Innsbruck

Later in February, 14th-24th, Elham was invited by Professor Keiji Matsumoto, to visit his quantum information group at the National Institute of Informatics (NII), Tokyo, **Japan**. Elham collaborated with Matsumoto on quantum languages and set up a new project on designing secure protocols with graph states.



Trip South to USA

Jonathan Baugh (left) and Colm Ryan attended the 4th ENC Conference (Experimental Nuclear Magnetic Resonance Conference) which was held April 10th-15th in Providence, Rhode Island. Both Colm and Jonathan presented posters of their work at the poster sessions. They also visited David Cory's NMR lab at MIT.



Rhode Island Convention Center

Page 9 of 12



MEDIA

Cercatella diana Teran Recall on alla September

SECTION B



AGE OF TAME AN COMPANY ALL DRAWN

BOTTOM AND DESITES - BE-BT

Judge Both teacher only 'ossueked' kick to handle autistic boy's tantrum



UW, Laurier win \$32M in science grants

Rectar start

TENDERS

Access to a second

The part is the support prober of the support of th

On Saturday, May 7th, 2005, the Kitchener-Waterloo RECORD featured Colm Ryan's receipt of a federal grant from Science and Engineering Research Canada (NSERC). The article entitled "UW, Laurier win \$32M in science grants" declared Colm an "extremely bright student."



Proposed IQC-Nano Building



Page 10 of 12



VISITORS



April 22, 2005

Shyamala B. Cowsik, *The Indian High Commissioner,* is a professional diplomat with a Master's degree in Physics. She joined the Indian Foreign Service after being the first woman to top the Civil Services examination. Ms. Cowsik has served at Geneva, Washington, Bangkok, Belgrade, the Philippines, Cyprus, the Netherlands and now she serves as the Ambassador of India to Canada.

2005

January 2005

January 4-12 Renato Renner Insitute of Theoretical Computer Science, Haldeneggsteig, Zurich

January 10 Paul Haljan Department of Physics, University of Michigan

January 18-February 10 Matthias Christandi Cambridge University

January 19 Jean Bedard

January 20 Sheueling Chang Sun Microsystems

January 21 Jim Mitchell Sun Microsystems

January 24

Karol Zyczkowski Centre for Theoretical Physics, Polish Academy and Institute of Physics, Jageillonian University January 26 Geordie Rose D-Wave Systems .

February 2005

February 9 & 16 Daniel Lidar University of Toronto

February 14-18 Robert Raussendorf Caltech

February 27-March 3 Alexander Shnirman Institut für Theoretishce Feskörperphysik Universität Karlsruhe

March 2005

March 3 Gilles Brasard Universite de Montreal

March 3 Anton Zeilinger University of Vienna

March 10 Danish Media Mission

March 14 Alain Aspect Institue d'Optique, France March 15 Thomas Frostberg Swedish Media

March 14-17 Norbert Lutkenhaus Friedrich-Alexander University

March 17-18 David Cory MIT

March 20-23 Paul Haljan University of Michigan

March 28-31 Andrew White Queensland University, Australia

April 2005

April 4-6 Frank Wilhelm CENS Ludwig-Maximilians-Universitat

April 4-8 Lawrence loannou Cambridge University

April 5 **Kenny Patterson** University of London April 7-8 **David Cory** MIT

April 11-13 Adam Hubbard Walla Walla College Washington

April 13 Seth Lloyd MIT

April 13-16 Will Oliver MIT

April 14 Adrian Kent Cambridge-DAMPT

April 18 Brian Eno

April 18-19 March Feldman University of Rochester

April 22 Shyamala B. Cowsik Indian High Commissioner

April 22 Oleksiy Pikalo BBN Technologies





A special thanks to Mike Lazaridis for having the vision, and providing the support that led to the creation of this institute.









