IQC

The Quantum Revolution **Starts Here**

ANNUAL REPORT | 2010

INSTITUTE FOR QUANTUM COMPUTING | UNIVERSITY OF WATERLOO

“Any sufficiently advanced technology is indistinguishable from magic.”

Arthur C. Clarke

Quantum mechanics can seem so strange and counter-intuitive, Einstein himself described its effects as “spooky.”

The atomic realm — where objects exist in two places simultaneously, and can be altered merely by being observed — obeys its own set of rules, which require us to think differently about our world and ourselves.

Thinking differently is the common thread that connects all the revolutionary research being conducted at the Institute for Quantum Computing.

IQC’s leading-edge scientists are exploring and taming the quantum building blocks of nature, paving the way for previously unimaginable technologies that will transform the ways we work, play, think and live.

Advancements such as ultra-powerful computers and unbreakable cryptography might seem like magic, but in the quantum era, such possibilities no longer demand a leap of faith.

Take the quantum leap with IQC.

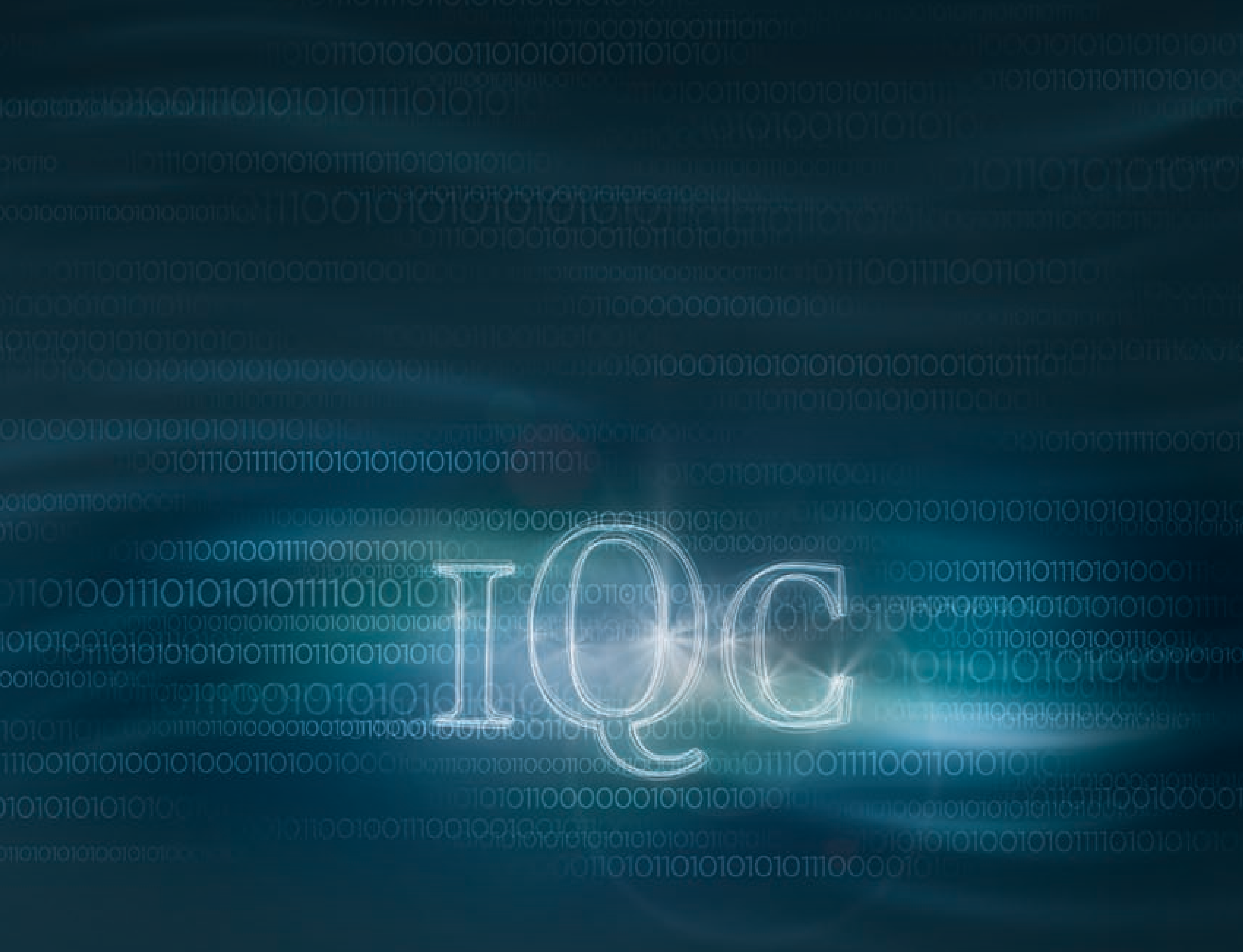


TABLE OF CONTENTS

Welcome to the quantum era

A message from the
EXECUTIVE DIRECTOR

THROUGHOUT HISTORY, SOCIETY HAS BEEN CONTINUALLY TRANSFORMED BY HUMANKIND'S ABILITY TO HARNESS THE LAWS OF NATURE, FROM FIRE TO STEAM TO ELECTROMAGNETISM AND MORE. INNATE HUMAN CURIOSITY — OUR INSATIABLE DESIRE TO UNDERSTAND AND IMPROVE OUR WORLD — HAS ALWAYS BEEN THE DRIVING FORCE BEHIND SCIENCE, TECHNOLOGY AND INNOVATION.

This curiosity has now inspired us to look at nature's most fundamental building blocks — those of the quantum realm — and envision how they will transform the lives of our children and grandchildren. We have only dipped our toes into the vast quantum sea, but already we know quantum technologies have the potential to change everything.

The Institute for Quantum Computing at the University of Waterloo was created to pave the way into this quantum future. IQC's mission is to conduct world-leading quantum information science, attract the world's top quantum scientists to Waterloo, educate the next generation of researchers, and become the authoritative source for commentary and analysis on this exciting branch of science. We strive to prepare the workforce and the world for the amazing possibilities of quantum information processing.

Since IQC's inception eight years ago, our growth can be best described using a term that frequently pops up in conversations about quantum computing: exponential. Our scientific scope, our stellar personnel and our international renown have continually redoubled. Today IQC has a complement of 17 faculty members, 25 postdoctoral fellows and 63 students, making IQC the largest institution of its kind in the world, with much more growth still to come.

Next year, IQC will expand into the Mike and Ophelia Lazaridis Quantum-Nano Centre, at the heart of the University of Waterloo campus. The state-of-the-art facility will catalyze new discoveries and foster collaboration between IQC researchers and colleagues within the University of Waterloo's many exceptional faculties and departments. Built to the most stringent standards for experimental quantum research, the building will continue the university's long tradition of being a magnet for the world's brightest minds.

IQC's successes, both past and yet-to-come, would be impossible without the remarkable support we have received from donors and partnerships, both public and private. The philanthropy and vision of Mike and Ophelia Lazaridis, along with invaluable backing from the federal and provincial governments, have turned IQC from an idea into a reality. I am grateful to the University of Waterloo for providing the support and fertile intellectual ground in which IQC has grown. Of course, I am inestimably grateful to the dedicated researchers, students and staff who make great science come to life at IQC every day.

This report will give you a taste of why I'm so excited about IQC. Within the coming pages, we'll give you a taste of the amazing breakthroughs and possibilities that lie ahead. I truly believe the work being done at IQC will have an incalculable impact — not only on science, but on society as a whole.

Raymond Laflamme | Executive Director, IQC

Leading the charge

A message from the
BOARD CHAIR

SINCE ITS CREATION BY THE UNIVERSITY OF WATERLOO LESS THAN A DECADE AGO, IQC HAS ESTABLISHED ITS EXCELLENCE IN THE FIELD OF QUANTUM INFORMATION. IN THE PAST YEAR ALONE, THE INSTITUTE HAS SET LOFTY GOALS FOR ITSELF — SPANNING RESEARCH, EDUCATION, RECRUITMENT AND OUTREACH — AND MADE REMARKABLE STRIDES TO ACHIEVE THOSE GOALS.

This success is evidence of the dedication and passion of the outstanding people at IQC. I see the faculty, the students and the staff motivated by the vision of excellence and leadership in the global quantum revolution.

In May 2010, IQC welcomed Dr. David Cory, a pioneer in his field and a long-time research collaborator with IQC, as the Canada Excellence Research Chair in Quantum Information. As one of 19 such Chairs appointed at institutions across Canada, Cory will bring a wealth of new knowledge and insight to IQC.

New to IQC's Board of Directors is Cosimo Fiorenza, whose vast knowledge and experience in Canadian law and business, and his deep commitment to research, make him an invaluable asset to IQC and its Board.

Of course, the future of quantum information processing lies in the hands of the exceptional graduate students and postdoctoral fellows who continue to bring fresh insights and energy to IQC.

The creation of a new collaborative graduate studies program in quantum information — a wonderful achievement spearheaded by IQC Deputy Director Michele Mosca — is particularly important. It will offer the next generation of quantum scientists at Waterloo an incredible education in their chosen field.

Of course, IQC will always owe a debt of gratitude to Mike Lazaridis, whose vision, passion and outstanding generosity made IQC possible in the first place. We are also very grateful for the unswerving support from the University of Waterloo, under the leadership of President David Johnston.

Last but certainly not least, I must express the Board's enormous respect and admiration for Raymond Laflamme. His visionary leadership as IQC's director, and his personal accomplishments as a quantum information scientist, have been the driving force behind the institute's many achievements.

On behalf of the Board of Directors, I thank and commend the faculty, students and staff at IQC for their splendid work in establishing Canada's place at the forefront of the next transformative technology, quantum information processing.

I look forward with excitement and optimism to what the people of IQC will achieve in the coming years.

Tom Brzustowski
Chair of the Board of Directors, IQC

Overview of IQC

OUR MISSION IS TO DEVELOP AND ADVANCE QUANTUM INFORMATION SCIENCE AND TECHNOLOGY AT THE HIGHEST INTERNATIONAL LEVEL THROUGH THE COLLABORATION OF COMPUTER SCIENTISTS, ENGINEERS, MATHEMATICIANS AND PHYSICAL SCIENTISTS.

Strategic objectives

1 To establish Waterloo as a world-class centre for research in quantum technologies and their applications

2 To become a magnet for highly qualified personnel in the field of quantum information

3 To establish IQC as the authoritative source of insight, analysis and commentary on quantum information

Who we are

IQC is a scientific research institute at the University of Waterloo exploring and taming the quantum universe to transform information processing. The institute's researchers are in the Faculties of Mathematics, Science and Engineering at the University of Waterloo.

What we do

IQC has assembled a critical mass of researchers and students pursuing a wide variety of theoretical and experimental approaches to quantum information. IQC will continue to build a vibrant knowledge community of researchers who will help establish Waterloo and Canada as global leaders in the quantum information revolution.

OUR VISION: HARNESSING QUANTUM MECHANICS WILL LEAD TO TRANSFORMATIONAL TECHNOLOGIES THAT WILL BENEFIT SOCIETY AND BECOME A NEW ENGINE OF ECONOMIC DEVELOPMENT IN THE 21ST CENTURY.

"In less than a decade, IQC has grown from a single big idea to a world-class research centre. This tremendous success would not have been possible without the vision and generosity of Mike and Ophelia Lazaridis. Their financial contributions of more than $100 million have been instrumental in putting IQC at the forefront of quantum information science."

Raymond Laflamme,
Executive Director, IQC

How we got here

The idea of creating a quantum information research institute in Waterloo emerged in the fall of 2000 during discussions between Mike Lazaridis, Professor Michele Mosca and Howard Burton.

Lazaridis, co-founder and co-CEO of Research in Motion, had already demonstrated his vision for scientific excellence in Waterloo with a donation of $100 million toward the Perimeter Institute for Theoretical Physics (PI). Mosca, a University of Waterloo professor and founding researcher at PI, was determined to foster high-level research in the emerging field of quantum information science. Burton, founding executive director of PI, was in the midst of recruiting one of the world's leading experts in quantum computing, Raymond Laflamme.

Lazaridis, Mosca and Burton envisioned the potential of creating a large-scale organization dedicated to researching the theory and implementations of quantum computing. Collaborations between Lazaridis and University of Waterloo President David Johnston, turned the vision into reality.

Thanks to more than $100 million in funding from Mike and Ophelia Lazaridis, combined with roughly $200 million in support from federal, provincial and private agencies, IQC is achieving its mission of conducting quantum information research at the highest international level.

IQC and the Quantum Revolution

Computers have steadily become smaller and more powerful over the past half-century. This trend is encapsulated in Moore's Law (named for Intel co-founder Gordon Moore), which states that the size of computer transistors shrinks by half every 18 to 24 months. Moore's Law has held true for decades, but the miniaturization of transistors is now reaching a critical threshold: at this rate, transistors will soon be the size of single atoms.

At such a tiny scale, the rules of physics suddenly change from "classical" to "quantum" — a whole new ball game. Researchers are working to create new computers that not only obey these laws but harness and capitalize on them to change the ways we work, communicate and live.

IQC's unique environment fosters cross-disciplinary collaboration between researchers at the forefront of this emerging science. The quantum information revolution has begun, and IQC is poised to lead Canada and the world into this exciting future. ■

Research focus

THE RESEARCH AT IQC IS AIMED AT HARNESSING THE QUANTUM WORLD AND TRANSFORMING THE SCIENTIFIC AND INDUSTRIAL LANDSCAPE. At the deepest level of the atomic world, the laws of physics are governed by quantum mechanics, which imposes fundamental physical limits to controlling systems. The development of quantum sensors, quantum communications and quantum information systems will push these physical limits. The development of practical quantum sensors and actuators will find its first applications in the realm of nanotechnology as tools for navigating and controlling the nanoscopic world. As we harness the quantum world, quantum computers will become reality.

IQC's research breadth spans from the foundations of quantum information science to the development of quantum technologies; some experiments focus on the nano-scale, while others work on the planetary scale via satellite. Below are some of the areas of specialization explored by IQC's theoretical and experimental scientists.

Quantum Information & Communication

Computers have steadily become smaller and more powerful over the past half-century, thanks to the miniaturization of transistors. But as ever-shrinking technology crosses the threshold into the atomic realm, the laws of quantum physics suddenly take hold. While this poses serious hurdles for classical computing, it opens incredible new possibilities in the realm of quantum computing.

Classical computers use binary "bits" of ones and zeros. Quantum computers will encode such bits in physical systems where we can also harness the quantum mechanical properties and obtain a more powerful system of quantum bits, or qubits. Thanks to the amazing rules of quantum mechanics, qubits can be in a "superposition" of zero and one simultaneously. Another quantum property called "entanglement," which Einstein and others debated decades ago, has since been harnessed in laboratories, and allows us to achieve tasks such as quantum teleportation and squeezing two bits of classical information into a single qubit. Quantum teleportation allows a qubit of information to be transmitted over a distance (indeed, teleported) by sending only two bits of classical information, and has important applications in quantum communication and building robust quantum computers.

IQC faculty members are exploring the fundamental properties of quantum information. Ashwin Nayak has led pioneering work in quantum coding with random access codes. Debbie Leung's work has contributed to the refutation of the "additivity conjecture" for quantum channel capacities. Norbert Lütkenhaus, Richard Cleve and John Watrous have made significant discoveries in the theory of communication using qubits.

Prof. Norbert Lütkenhaus

Quantum Algorithms & Complexity

The field of quantum computing was kick-started in the 1980s when it was discovered that certain computational problems can be tackled more efficiently with quantum algorithms than with their classical counterparts. The most prominent such breakthrough came when MIT researcher Peter Shor (then at AT&T) unveiled an algorithm that could efficiently factor very large numbers — a feat believed to be impossible for classical computers. Since then, an increasing number of difficult computing tasks, such as "needle-in-haystack" search problems, have been shown to be sped up with quantum algorithms.

Whereas algorithms focus on what a quantum computer can achieve, the study of complexity examines how well they can (or cannot) achieve these tasks. Quantum complexity examines the concept of difficulty — the "hardness" of certain problems to solve. In 2009, John Watrous and collaborators achieved a major breakthrough when they resolved a decade-old complexity problem by proving the equivalence of two collections of computational problems called QIP and PSPACE. Contributions that have shaped the field have also been made by IQC faculty including Andrew Childs, Richard Cleve, Michele Mosca, Ashwin Nayak and Ben Reichardt.

faculty

NEW FACULTY MEMBER

DR. DAVID CORY

Dr. David Cory joined IQC in June 2010 as Canada Excellence Research Chair (CERC) in Quantum Information Processing. Cory comes to IQC following a tenure as professor of nuclear engineering at Massachusetts Institute of Technology. Cory will lead new experimental investigations into quantum sensors and actuators — the building blocks of future quantum computers. He has described IQC as a "wonderful environment" in which to pursue this leading-edge research, and lauded the Canadian government for investing in such important work.

"This chair will provide the resources needed to design, fabricate and test a first generation of quantum devices," Cory said. "Over the past decade, the engineering of quantum systems has become a reality. Now we aim to deploy quantum devices." Cory's IQC laboratory in the new Research Advancement Centre 2 (RAC2) contains state-of-the-art equipment for conducting experiments using nuclear spin, electron spin, superconducting qubits and quantum optics.

His research is expected to contribute to the world's first generation of practical quantum devices. These new technologies will have immediate and future applications in medicine, communications, biochemistry, physics and nanoscience. Said IQC Director Raymond Laflamme: "With a scientist the calibre of David Cory as CERC Chair, Canada will be even better positioned to lead the world in the quantum information revolution."

DR. JONATHAN BAUGH

Dr. Jonathan Baugh joined IQC in 2007 and is a professor in the University of Waterloo's Chemistry Department. As group leader in the laboratory for quantum spintronics, Baugh is working toward the physical realization of quantum information processors in solid-state systems. He and his research group are developing prototypes and the quantum control techniques necessary for scalable quantum information processing. His focus is on single electronic spins in quantum dots, combined electron-nuclear spin systems and solid-state nuclear magnetic resonance.

DR. ANDREW CHILDS

Dr. Andrew Childs joined IQC in 2007 and is a professor in the University of Waterloo's Department of Combinatorics and Optimization. His research is focused on the theory of quantum information processing with particular emphasis on algorithms for quantum computers. His interests include continuous-time algebraic problems, such as the hidden subgroup problem, and quantum query complexity. His contributions to the development of quantum walk algorithms include an example of exponential speedup over classical computation, algorithms for locally searching graphs, and a nearly optimal algorithm for evaluating AND-OR formulas.

DR. RICHARD CLEVE

Dr. Richard Cleve joined IQC in 2004 and holds the IQC Endowed Chair in Quantum Computing. He is a professor in the University of Waterloo's School of Computer Science. Cleve has made significant contributions to quantum algorithms and information theory including simplifications and improvements on existing quantum algorithms. He has also been involved in the development of novel algorithmic paradigms, such as quantum walks.

Research focus

Quantum Cryptography

Every time you perform an online transaction, such as a purchase or bank transfer, you entrust your personal data to a secure encryption system. Such encryption is based on mathematical problems too difficult for present-day computers to crack, which is why your information is relatively safe. But future computers — quantum computers in particular — will be able to decrypt many such coded messages. We need new cryptographic tools that are secure in a quantum world. Fortunately, the rules of quantum mechanics enable codes that cannot be broken with any amount of computing power.

The rules of quantum mechanics dictate that a quantum system cannot be observed without being disrupted. This means that "key" material exchanged via quantum communication will bear the indelible fingerprint of any attempted eavesdropping. Eavesdropped keys can be abandoned, and only truly private keys are kept to be used in unbreakable encryption protocols. IQC is home to Alice, a photon receiver in a Quantum Key Distribution system. Alice's counterpart, Bob, is housed in an office at Waterloo's Perimeter Institute for Theoretical Physics. Alice and Bob receive entangled (highly correlated) photons emitted from a crystal excited by a laser. By measuring the unique polarization of the photons, Alice and Bob receive random (but identical) "keys," which can be used to encode messages. IQC researcher Norbert Lütkenhaus is a leading international authority on the security of practical quantum key distribution systems. Thomas Jennewein is a world leader in quantum communication and quantum cryptography in free space. IQC researchers including Richard Cleve, Raymond Laflamme, Norbert Lütkenhaus, Debbie Leung, Michele Mosca and Ashwin Nayak have worked on this and other facets of quantum cryptography, such as quantum fingerprints, quantum money and quantum private channels.


IQC's quantum key distribution experiment, affectionately known as Alice

> "IQC has a track record of recruiting faculty of the highest calibre from the fields of physics, computer science, mathematics and engineering. With a critical mass of both experimentalists and theorists, IQC tackles the big questions of quantum information science at a level second-to-none in the world."
>
> **Michele Mosca**
> *Deputy Director, IQC*

Quantum Error Correction & Fault Tolerance

One of the biggest hurdles faced by quantum computing researchers is called decoherence — the tendency of quantum systems to be disturbed. This vulnerability to noise leads to errors, which can be overcome by Quantum Error Correction. Because error correction techniques are themselves susceptible to noise, it is crucial to develop fault-tolerant correction.

IQC Director Raymond Laflamme is one of the pioneers of quantum error correction and the theory of fault-tolerant quantum computing. In collaboration with new IQC faculty member David Cory, Laflamme conducted the first experimental testing of quantum error correction in liquid-state nuclear magnetic resonance. IQC faculty members Joseph Emerson, Ben Reichardt, Frank Wilhelm and Debbie Leung have all made significant contributions to the field, including: noise characterization, decoherence theory, control theory and approximate quantum error correction.

faculty

Spin-Based Quantum Information Processing

A well-known technology that has long been used in biomedical imaging also serves as a natural test-bed for quantum computing. Nuclear Magnetic Resonance (NMR) manipulates the quantum states of nuclear "spins" in molecules. Because the nuclei behave like tiny magnets, they can be controlled and manipulated using magnetic fields and radiofrequency pulses — and thus serve as qubits. So far, NMR has been the most successful system in implementing quantum algorithms.

A team of researchers led by IQC faculty Raymond Laflamme and David Cory hold the current record for the most well-characterized qubits harnessed in a single experiment (12). Other IQC faculty including Jonathan Baugh, Joseph Emerson, Debbie Leung, and Michele Mosca have also made numerous critical contributions to the development of spin-based quantum computing.

Future research will require a platform that can be scaled up to harness an increasing number of qubits. Trapping and controlling single electron spins in nanoscale devices (such as point defects, quantum wires or semiconductor quantum dots) is at the heart of research done by IQC researchers Jonathan Baugh and David Cory. Creating a viable system with many qubits is key to realizing the full power of quantum information processing.

Prof. Jonathan Baugh working in the Spintronics lab

DR. JOSEPH EMERSON

Dr. Joseph Emerson joined IQC in 2005 and is a professor in the University of Waterloo's Department of Applied Mathematics. Emerson's current primary research focus is the development of randomization methods for assessing the performance of quantum information devices in the presence of errors, a key step toward making large-scale quantum information processors viable. Emerson is also an affiliate member of Perimeter Institute.

DR. THOMAS JENNEWEIN

Dr. Thomas Jennewein joined IQC in 2009 and is a professor in the University of Waterloo's Department of Physics and Astronomy. His current research centres on the applications of quantum photonics and quantum optics, as well as the fundamental aspects of the quantum world. He is involved in the experimental design of devices based on quantum photonics suitable for communication and computing with photons, and the development of long-distance quantum communication systems using terrestrial and satellite-based systems.

DR. RAYMOND LAFLAMME

Dr. Raymond Laflamme is the founding director of IQC and a founding member of Perimeter Institute. Laflamme is also the founding scientific director of QuantumWorks, Canada's national research consortium on quantum information science. Laflamme holds the Canada Research Chair in Quantum Information, and is a Professor in the Department of Physics and Astronomy at the University of Waterloo. He completed his PhD on aspects of general relativity and quantum cosmology under the direction of Stephen Hawking. Laflamme is a pioneer in the field of quantum error correction, and along with his research group he holds the world record for the largest quantum computer achieved to date, 12 qubits.

DR. DEBBIE LEUNG

Dr. Debbie Leung joined IQC in 2005 and is a professor in the University of Waterloo's Department of Combinatorics and Optimization. She holds the Canada Research Chair in Quantum Communication, is a member of the Canadian Institute for Advanced Research (CIFAR) Quantum Information Processing Program. She completed her PhD in Physics at Stanford.

DR. ADRIAN LUPAŞCU

Dr. Adrian Lupaşcu joined IQC in 2009 and is a professor in the University of Waterloo's Department of Physics and Astronomy. He works on superconducting atom-chips, Rydberg atoms and superconducting charged particle detectors. He completed his PhD at the Delft University of Technology in the Netherlands, where his thesis research involved experiments on dispersive measurement of superconducting qubits. Lupaşcu's work at IQC focuses on superconducting qubits and the interaction between artificial atoms and light at microwave frequencies.

DR. NORBERT LÜTKENHAUS

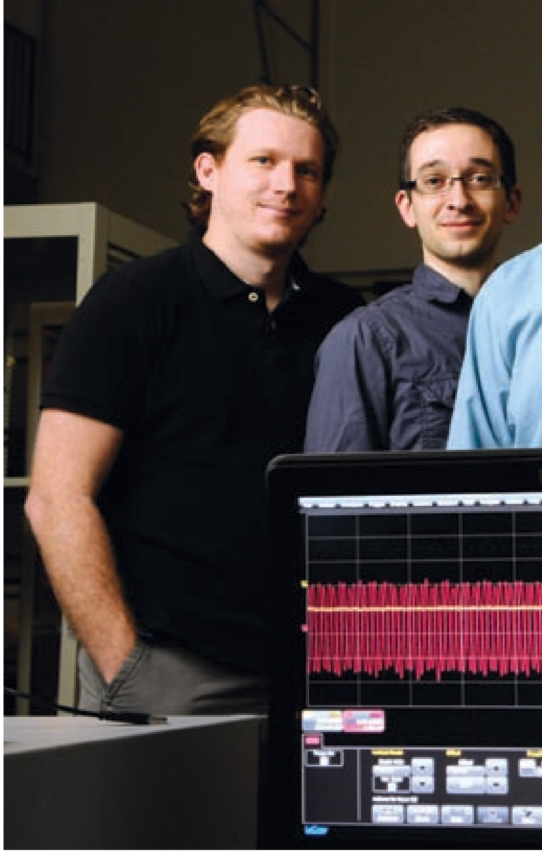
Dr. Norbert Lütkenhaus joined IQC in 2006 and is a professor in the University of Waterloo's Department of Physics and Astronomy. He is also a member of the university's Centre for Applied Cryptographic Research (CACR), an Affiliate Member of the Perimeter Institute, and a member of QuantumWorks, Canada's national research consortium on quantum information science. Lütkenhaus has made key contributions to the theory and practice of quantum information technology and quantum cryptography.

DR. HAMED MAJEDI

Dr. Hamed Majedi joined IQC in 2005 and is a professor in the University of Waterloo's Department of Electrical and Computer Engineering and the department of Physics and Astronomy. Majedi established the institute's Integrated Quantum Optoelectronics Laboratory (IQOL) for the characterization of superconducting and photonic quantum devices, focusing on the development of a superconducting single-photon detector in the infrared range.

Research focus

Nanoelectronics-Based Quantum Information Processing



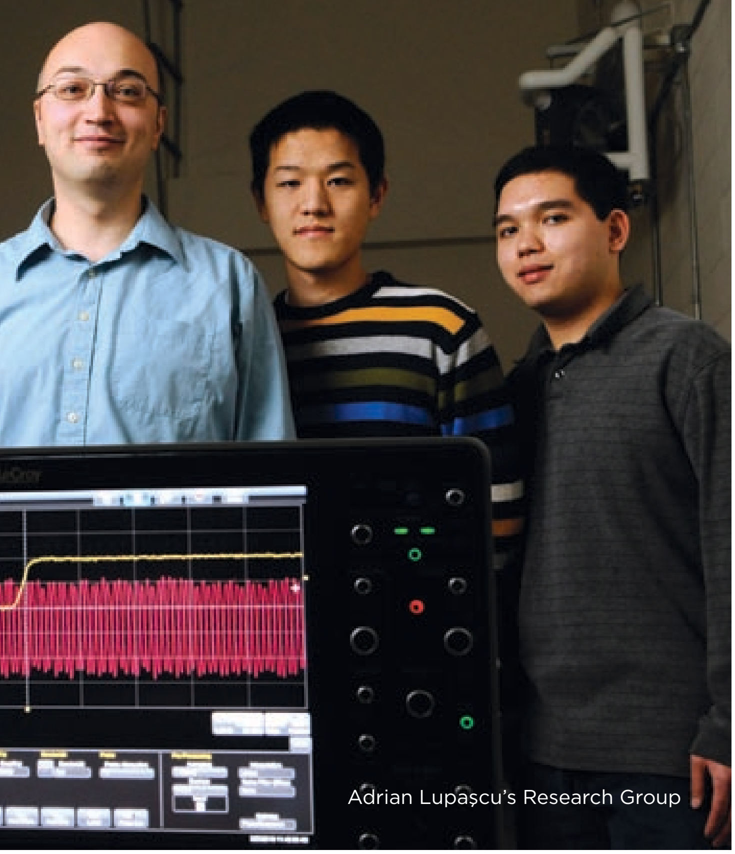
Because they are based on standard semiconductor technology, nanoscale systems such as quantum dots and superconducting circuits make good candidates for practical quantum computers. Once a few such systems are shown to work above a given threshold, the key will be to make them work together in scalable technology. Significant progress has been made in reducing errors, implementing algorithms and observing entanglement using these systems. IQC is home to two new labs in these fields: the Quantum Spintronics laboratory and the Superconducting Quantum Devices laboratory. IQC theorists and experimentalists including Frank Wilhelm, Jonathan Baugh, Adrian Lupaşcu and Hamed Majedi are leading these investigations. Their work will be essential as quantum information technology moves closer toward practical realization and commercialization.

Optical Quantum Information Processing


Students working in the Quantum Optics & Quantum Information lab

In quantum optics, photons (particles of light) are used to carry quantum information. Each photon has a polarization — for instance, vertical or horizontal, which can be ascribed with the classic bit states of zero and one, respectively. But polarization can also be in a quantum superposition of these states — essentially zero and one at the same time. Since the means of manipulating the polarization of photons are well understood and easily achievable, optics makes an ideal test-bed for investigating quantum information processing. Some of the first realizations of novel quantum effects, such as teleportation and quantum key distribution, were achieved through optics research.

The seminal proposal by Emanuel Knill, Raymond Laflamme and Gerard Milburn (the KLM proposal) allows universal and scalable optical quantum computing using only single photons, linear optics and measurement. IQC faculty member Norbert Lütkenhaus has conducted leading research into such areas as entanglement verification and quantum logic operation. The team led by Kevin Resch focuses on fundamental experiments of quantum communication and algorithms, while Thomas Jennewein's optical research team investigates quantum communication through free space via satellite.



Adrian Lupașcu's Research Group

Quantum Sensors

Quantum information processing promises not only breakthroughs for computing, communications and cryptography, but it can also help us devise tools for navigating and controlling the nano-scale world. Sensors and actuators that operate according to quantum mechanics will achieve sensitivity, selectivity, precision and robustness far beyond their classical counterparts.

IQC faculty member David Cory's research in this area has included the improvement of neutron interferometry (NI), in collaboration with the National Institute of Standards and Technology (NIST) in Maryland. The development of interferometers inspired by quantum error correction techniques has already resulted in greatly enhanced robustness and permitted the design of special purpose NI for new applications to magnetic and soft matter. Quantum actuators currently under development in Cory's lab include electron spin control of nuclear spins, electron spin control of transport, optical control of electron and nuclear spins, and electron spin control of superconducting circuits. Ultimately, this research aims to integrate quantum sensors and actuators into more complex systems and achieve higher levels of functionality. These complex systems could be used, for example, to detect single spins or even serve as building blocks for the development of practical quantum information processors. ■

faculty

DR. MICHELE MOSCA

Dr. Michele Mosca is co-founder and the Deputy Director of IQC and is a professor in the University of Waterloo's Department of Combinatorics and Optimization as well as the departments of Computer Science and Physics and Astronomy. Mosca is also a founding member of the Perimeter Institute and has made major contributions to the theory and practice of quantum information processing, particularly in the areas of quantum algorithms, quantum self-testing and private quantum channels. Mosca holds the position of Canada Research Chair in Quantum Information.

DR. ASHWIN NAYAK

Dr. Ashwin Nayak joined IQC in 2002 and is a professor in the University of Waterloo's Department of Combinatorics and Optimization. He is also a Scholar at the Canadian Institute for Advanced Research. He earned his PhD in computer science from University of California, Berkeley in 1999, and completed a postdoctoral fellowship at the DIMACS Center (Rutgers University) and AT&T Labs-Research. He has made several key contributions to the understanding of quantum computational complexity.

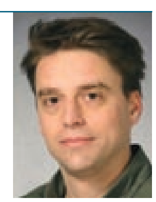
DR. BEN REICHARDT

Dr. Ben Reichardt joined IQC in 2008, and is a professor in the University of Waterloo's School of Computer Science. After completing his undergraduate degree at Stanford University, he earned a PhD in computer science at the University of California, Berkeley. In his doctoral work, he gave the first proof that fault-tolerance schemes based on noise detection could function in the presence of noise. Reichardt studies quantum fault tolerance and quantum algorithms, and his work brings together ideas from theoretical computer science and quantum physics.

DR. KEVIN RESCH

Dr. Kevin Resch joined IQC in 2006 and is a professor in the University of Waterloo's Department of Physics and Astronomy. He completed his PhD at the University of Toronto in 2002, focusing on experimental quantum optics. In 2003, Resch was involved in building the first free-space quantum communication link for entangled photons. He now heads the research group working in IQC's Quantum Optics Laboratory, investigating the generation and characterization of quantum states of light.

DR. JOHN WATROUS



Dr. John Watrous joined IQC in 2006 and is a professor in the University of Waterloo's School of Computer Science. In 2008 he was named a Fellow at the Canadian Institute for Advanced Research (CIFAR) Quantum Information Processing Program. Watrous and collaborators achieved a major breakthrough in 2009 when they resolved a decade-old complexity problem by proving the equivalence of two collections of computational problems called QIP and PSPACE.

DR. FRANK WILHELM

Dr. Frank Wilhelm joined IQC in 2006 and is a professor in the University of Waterloo's Department of Physics and Astronomy. Prior to arriving at IQC he was a lecturer at Ludwig-Maximilians University in Munich. He earned his doctorate in physics at the University of Karlsruhe in Germany in 1999. Wilhelm's major contributions include the proposal of the first practical electronically controllable qubit-qubit interactions, the proposal of macroscopic dynamical quantum tunneling, and the introduction of optimal control theory to the physics of solid-state qubits. ■

Postdoctoral Fellows

2009/2010
Postdoctoral Fellows

Working alongside IQC's faculty and students are 25 postdoctoral fellows, whose expertise and innovative approaches to research enrich the institute's scientific landscape. These exceptional minds contribute to every aspect of IQC's mission, spanning research, publications, teaching and outreach. They represent the next wave of leaders in the field of quantum information science.

Gorjan Alagic, Dominic Berry, Anne Broadbent, Bill Coish, Alexander De Souza

Jay Gambetta, Gus Gutoski, Hannes Hübel, Lawrence Ioannou, Tsuyoshi Ito

Rainer Kaltenbaek, Xiongfeng Ma, Will Matthews, Seth Merkel, Marco Piani

Robert Prevedel, Mohsen Rasavi, Colm Ryan, Simone Severini, Urbasi Sinha

Yipu Song, Tzu-Chieh Wei, Zhizhong Yan, Bei Zeng, Jingfu Zhang

Anne Broadbent

Photo by Peter Lee courtesy of *The Waterloo Region Record*

Anne Broadbent, a postdoctoral fellow at the Institute for Quantum Computing, finds balance between her leading-edge scientific research and her family life on a 10-acre farm nicknamed Windy Poplars.

In a feature published in *The Waterloo Region Record*, Broadbent said mathematics has an "elegance" that has always attracted her, not unlike the rustic beauty of her homestead northwest of Waterloo.

Broadbent introduced readers to her husband, Didier Guignard, their seven-month-old son Danny, and the family pet — a Bernese mountain dog named Berny.

The article was an instalment of a Record series called Young Innovators, which profiles the next generation of leading-edge thinkers in Waterloo Region. Further instalments are scheduled to include profiles of IQC postdoctoral fellows including Bill Coish and Urbasi Sinha.

The feature about Broadbent traces her path from her Ottawa childhood to her young adulthood in Waterloo decoding (and creating) the secrets of cryptography.

She pursued cryptography during her PhD studies in Montreal, and soon thereafter began her postdoctoral fellowship at IQC.

In the newspaper article, Broadbent says her work at IQC allows her to be continually amazed by the "elegance and creativity" of mathematics.

"It's like putting together a puzzle, but you don't know what the final outcome will look like," she said. "These are the pieces, what can I build with them? Or sometimes, you think about building something, but it comes out slightly differently than you thought, but it is just as interesting, or more interesting."

Quantum Information Processing with Spins and Superconductors

IQC postdoctoral fellows Bill Coish and Jay Gambetta spearheaded an innovative, three-day workshop exploring quantum computing via spins and superconductors.

Titled Quantum Information Processing with Spins and Superconductors (QISS), the workshop was designed to foster an exchange of ideas and research between scientists working on superconducting systems and electron spins.

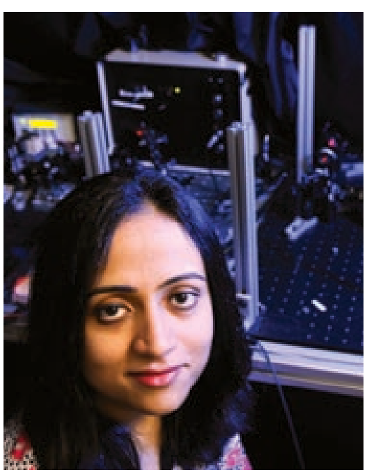
Held in May, the QISS workshop saw 17 guest speakers from North America, Europe and Japan deliver presentations to roughly 60 participants.

The workshop also included a poster session, which allowed IQC scientists with varied research interests to share their ideas and results with the invited guests.

Topics covered during QISS included: new designs for superconducting qubits, decoherence sources and error estimations, quantum information processing with solid-state systems, generating and measuring entanglement, and many more.

Coish and Gambetta deemed the workshop a big success, and plan to host it again in coming years.

Urbasi Sinha



A team led by IQC postdoctoral fellow Urbasi Sinha earned an article in the prestigious journal *Science* for fundamental research in quantum mechanics.

The paper puts one of the fundamental axioms of quantum mechanics, Born's rule, to the test. Born's rule, which gives the probability that a measurement on a quantum system will yield a given result, is widely assumed to always hold true.

This assumption is what led physicist W.H. Zurek to remark: **"If Born's rule fails, everything goes to hell."**

Sinha and her IQC colleagues sought to find out if everything could indeed go to hell.

They devised a variation to the famous "double-slit" experiment, which has long been used to demonstrate the counter-intuitive laws of quantum mechanics. Their "triple-slit experiment" aimed to test the fundamental postulates of quantum mechanics, on which other applied research is based.

If the photons in the triple-slit experiment demonstrated any unexpected results, it would mean quantum mechanics is only approximate, just as the double-slit experiment demonstrated that classical physics is only an approximation to the true law of nature.

Even a small violation of Born's rule would indicate that quantum mechanics is merely approximate, and would change physics as we know it. This would imply even more generalized versions of quantum mechanics, thus even leading to new ideas such as "super quantum computing."

The researchers discovered no such violation, however, allowing them to put a bound on expectations of quantum mechanics.

This result affirms quantum mechanics as a pillar of modern physics and opens up new avenues for exploring the fundamentals of quantum mechanics. ■

Graduate Program

A NEW GRADUATE PROGRAM IN QUANTUM INFORMATION WILL COMMENCE AT THE UNIVERSITY OF WATERLOO IN FALL 2010, OFFERING STUDENTS AN UNPRECEDENTED BREADTH OF STUDY IN THE EMERGING FIELD.

The graduate program will expose students to a wide range of advanced research projects and courses on the foundations, applications and implementations of quantum information processing.

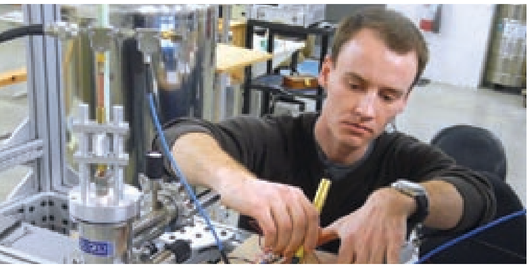
Applications are now being accepted for the program, which was created with consultation and approval from six academic units, three faculties and the university Senate.

One particularly special feature of the program is its scope, encompassing both experimental and theoretical aspects of quantum information. Students will be required to take two key courses: Quantum Information Processing and Implementation of Quantum Information Processing. They will have the opportunity to take a wide range of other specialized courses in quantum information, ranging from Theory of Quantum Information to Quantum Algorithms to Nanoelectronics Implementations of Quantum Information Processing.

"I don't know of any other program in the world where students acquire this depth of background in both the theory and implementation of quantum information," said IQC Deputy Director Michele Mosca, chair of the committee that oversees the program. "Students will be part of a world-renowned multi-disciplinary team of researchers harnessing the power of quantum mechanics."

Students will be based in their home program and earn a Quantum Information qualification to their degrees; for instance, Master of Mathematics in Computer Science (Quantum Information), or Doctor of Philosophy of Science in Chemistry (Quantum Information).

"The breakthroughs in quantum computing will likely happen across different disciplines," Mosca said. "We are sowing the seeds for that to happen. Big ideas tend to come from the cross-pollination of disciplines." ■



Jeremy Chamilliard

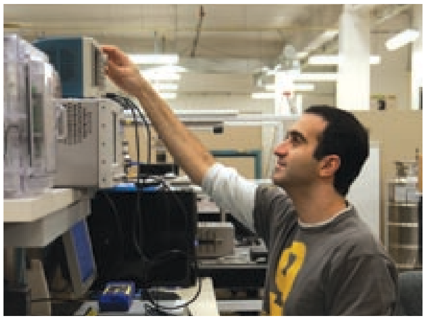
"Conducting my experimental research at IQC has provided me with the resources to acquire state-of-the-art equipment, the expertise to guide my work and the environment in which to carry out cutting-edge experiments in quantum information."

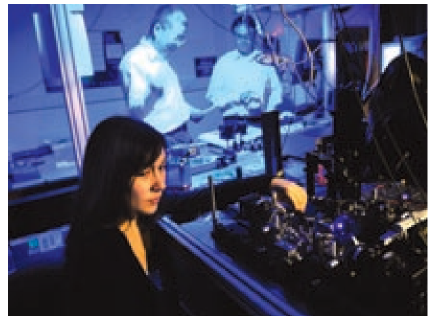
Easwar Magesan

"The interdisciplinary nature of IQC has broadened my scientific interests and provided me with the resources to pursue diverse areas of research. It is exciting to see the many important theoretical and experimental advances being made at the institute."

Gina Passante

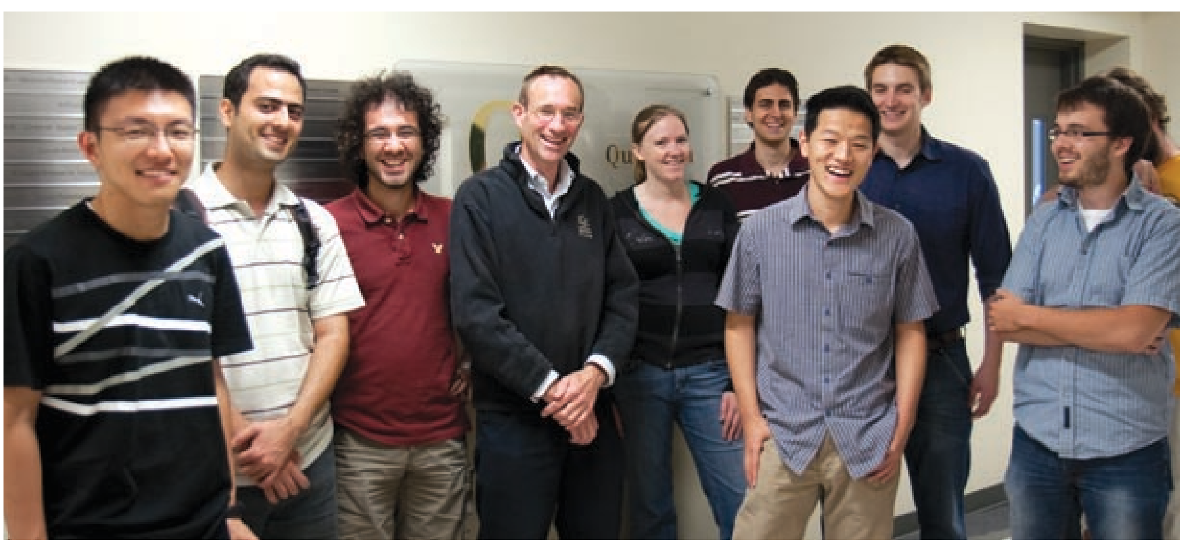
"Graduate studies in quantum information have given me the opportunity to learn about quantum information not only in my field of physics, but also from a mathematical and computer science point of view. When I leave IQC, I am certain that I will have a broader view of the field than if I had studied anywhere else."





Students

Jeyran Amirloo
Normand Beaudry
Devon Biggerstaff
Jean-Philippe Bourgoin
Jeremy Chamilliard
Alessandro Cosentino
Ben Criger
Pierre-Luc Dallaire-Demers
Chunqing Deng
Amin Eftekharian
Chris Erven
Agnes Ferenczi
Christopher Ferrie
Jennifer Fung
Behnood Ghamsari
MirMojtaba Gharibi
Sevag Gharibian
Peter Groszkowski
Deny Hamel
Tyler Holdon
Rolf Horn
Stacey Jeffery
Mohsen Keshavarz
Botan Khani
Milad Khoshnegar
Nathan Killoran
Robin Kothari
Jonathan Lavoie
Nicholas LeCompte
Chandrashekar Madaiah
Easwar Magesan
Laura Mancinska
Iman Marvian Mashhad
Thomas McConkey
Matthew McKague
Evan Meyer-Scott
Hamid Mohebbi
Ryan Morris
Felix Motzoi
Osama Moussa
Varun Narasimhachar
Christian Oppenlander
Jean-Luc Orgiazzi
Brendan Osberg
Yingkai Ouyang
Maris Ozols
Adam Paetznick
Gina Passante
David Pitkanen
Farzad Qassemi
Ansis Rosmanis
Bill Rosgen
Amir Jafari Salim
Kurt Schreiter
Cheng Shen
Lana Sheridan
Jamie Sikora
Jamie Smith
Jason T. Soo Hoo
Cozmin Ududec
Sarvagya Upadhyay
Rui Xian
Mike Zhang ■



“IQC will place Waterloo at the forefront of a new frontier of knowledge.”

David Johnston

President, University of Waterloo,
and Governor General Designate

The mission of IQC is to harness and control the very building blocks of nature — atoms, electrons, photons and the like — to revolutionize computing, communications and sensors. Because these building blocks obey the laws of quantum mechanics, they pose difficult challenges but promise tremendous potential rewards.

Over the next several pages, take a tour of IQC’s laboratories, and find out how researchers are taming the quantum world to develop the technology of the future.

“We consider IQC to be the best institute of its type in the world today.”

From an international NSERC-sponsored review panel in 2009

“IQC is arguably the leading achiever in the world in its field of endeavor, on all fronts.”

NSERC Panel Report, 2006

Take a tour of IQC

SUPERCONDUCTING QUBITS LAB. Harnessing quantum systems at the “mesoscopic scale” (~1μm) is possible by defining qubits using superconducting nano-devices embedded in electrical circuits (namely Josephson junctions which offer a scalable way to perform quantum computing). Scientists in this lab study the interaction between light and these qubits.

WELCOME TO IQC! Behind every door at IQC, researchers are investigating theoretical and experimental approaches to quantum information science. Until you can visit us in person, we invite you explore IQC in these pages.

Adrian Lupaşcu and Jason Soo Hoo working in the Superconducting Qubits Lab

THE THEORISTS. IQC’s theorists examine the potential power, scope and limits of quantum information processing. The mathematicians and computer scientists determine which computational tasks will be better tackled with quantum algorithms and how the principles of quantum mechanics can allow better communications and more secure cryptography. Theoretical physicists spend their time studying the challenges of physical implementation of QIP.

The quantum device theory group is working on a project funded by the Intelligence Advanced Research Projects Activity as part of an initiative for the United States government. The project is a collaborative effort between material scientists and physicists to investigate how to produce solid materials that are as free from imperfections as possible.

NUCLEAR MAGNETIC RESONANCE (NMR) LAB. The spin properties of nuclei are great candidates for qubits. Nuclear Magnetic Resonance has long been used in medical imaging and has proven a successful test-bed for early quantum computers. A research team from IQC and MIT holds the record for controlling the most qubits in any system, namely 12 in liquid-state. Solid-state NMR, using molecules held in a crystal rather than a liquid, poses new challenges but has the potential for faster control.

SOLID STATE QUANTUM DEVICE LAB. Inspired by the foundations of quantum mechanics and quantum information, this lab develops solid-state devices, such as sensors and actuators, designed to achieve greater efficiencies than are possible in the classical world. These first generation quantum devices will be the tools for navigating the nano-world and the building blocks of progressively more complex quantum processors.

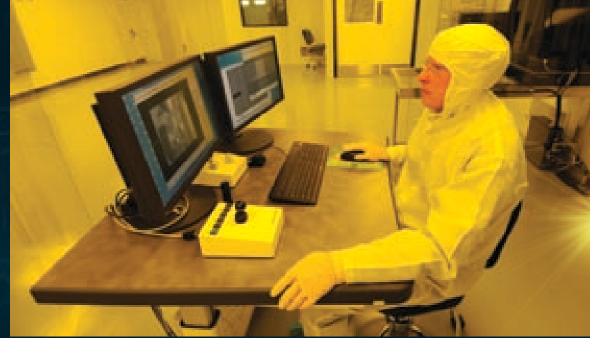
Researchers Kevin Resch, Jonathan Lavoie and Rainer Kaltenbaek explored classical analogues of two-photon quantum interference in *Physical Review Letters* paper published in June 2009.

COHERENT SPINTRONICS LAB. Although NMR and ESR can achieve impressive quantum control, it is challenging to add more qubits to these systems. Thanks to advances in semiconductor fabrication technologies, researchers can build very small (~100nm) "quantum dots" that can hold a single electron. The qubits are the electron spins confined using charged electrodes on nanowires.

IQC researchers Frank Wilhelm, Bill Coish and Farzad Qassemi examined how to deal with "blocks" to quantum computing in a May 2009 issue of *Physical Review Letters*.

ELECTRON SPIN RESONANCE (ESR) LAB. A natural extension to NMR is to use electron spins to control nuclear spins; this allows for faster operation while keeping the inherent robustness of the nuclear spins. These two systems demonstrate a high degree of control and are well-suited as test-bed quantum computer prototypes.

QUANTUM OPTICS AND QUANTUM INFORMATION LAB. Particles of light (photons) generated using lasers can be used as qubits. Photons interact very little with the environment, which makes them resistant to decoherence. Because creating entanglement between photons is important but difficult, research in this lab strives to find and characterize better sources of entangled photons and apply them to novel quantum information processing protocols. This lab also develops new technologies applicable to imaging.



CLEANROOM. IQC's fabrication cleanroom is certified Class 1,000, meaning that one cubic foot contains less than 1,000 particles (as opposed to the 1-5 million in typical outdoor air). Such conditions allow for use of the e-beam lithography system for patterning designs with dimensions as small as 20 billionths of a metre across. Other equipment, such as Atomic Layer Deposition and Optical Lithography, allows for the engineering of nano-scale devices.

INTEGRATED QUANTUM OPTOELECTRONICS LAB. One of the bigger challenges faced by researchers of optics-based quantum protocols is the actual detection of photons. Whether for communications or computing use, the future of quantum information research will require better, more accurate photon detectors. In this lab, researchers aim to develop and characterize a fast, high-efficiency photon detector that works at the frequency used to transmit photons in optical fibers.

GO ASK ALICE. "Alice" and "Bob" are photon receivers in IQC's "quantum key distribution" experiment. Thanks to quantum mechanical laws, tampering with the photon transmissions will be detectable when Alice and Bob measure their photons and publicly discuss a random selection of outcomes. As long as tampering is below a certain threshold, Alice and Bob can distil shared secret keys. With these keys, Alice and Bob may encrypt messages using unbreakable codes.

QUANTUM PHOTONICS LAB. The key goal pursued in this lab is to develop technologies that enable applications of quantum information and communication on a global scale. Researchers are developing technologies for quantum cryptography transmitted through optical fibres and free space to satellites. They are also engineering novel and high-quality states of entangled photons and applying them to quantum communication protocols and fundamental quantum physics experiments.

Mike and Ophelia Lazaridis Quantum-Nano Centre

"The new facility will create wonderful opportunities for scientists from many disciplines to chat, brainstorm and share ideas. Scientific breakthroughs often happen when great minds come together under one roof — which is exactly what we expect to happen at the QNC."

Raymond Laflamme
Executive Director, IQC


Construction site July 2010


KPMB Architects

QNC ground-breaking ceremony

> “Quantum Computing holds the promise of enabling computers with previously unimaginable power and accelerating fundamental research in quantum physics. We hope to see Waterloo become the epicentre of Quantum research and experimentation.”

Mike Lazaridis
Co-CEO, Research In Motion

The Mike and Ophelia Lazaridis Quantum-Nano Centre is under construction in the heart of the University of Waterloo’s main campus and is shared with the Waterloo Institute of Nanotechnology. The building was designed to foster cross-disciplinary collaboration between students and faculty and attract top scientists to the Waterloo area.

The building will include a suite of laboratories for research in quantum optics, NMR and ESR, quantum dots, superconducting qubits, coherent spintronics and quantum cryptography. It will also be adjacent to a new fabrication and metrology facility. The building was designed to meet the highest scientific standards including vibration, temperature, humidity and electromagnetic radiation standards.

The design of the QNC provides a focal point in the centre of the building that links all locations together in one main atrium. The layout is meant to bring mathematicians, computers scientists, chemists, physicists and engineers together and foster scientific interaction and collaboration.

IQC will have 125,000 sq. ft. at the QNC, which will provide office space for faculty and graduate students, research laboratories, fabrication and testing facilities, seminar and lecture rooms, numerous interaction spaces and a research seminar room which will accommodate up to 200 people.

The first of its kind in the world, the building will provide the space to nurture research, discussion and instruction in the exciting fields of quantum information and nanotechnology engineering. ■

The boomerang of life

Stephen Hawking visits IQC

Director Raymond Laflamme presents Prof. Hawking with the wooden boomerang

IQC WELCOMED THE WORLD'S MOST FAMOUS SCIENTIST, STEPHEN HAWKING, FOR A VISIT IN JUNE, 2010. Hawking spent an afternoon touring IQC's laboratories, meeting researchers and catching up with IQC Director Raymond Laflamme, who earned his PhD under Hawking's tutelage in the 1980s. As a memento of the visit, Laflamme presented his former mentor with a wooden boomerang — symbolizing one of the pair's earliest scientific collaborations. As a PhD student, Laflamme disproved Hawking's theory that time reverses direction in a contracting universe, leading Hawking to concede that "time is an arrow, not a boomerang." ■

University of Waterloo Provost Feridun Hamdullahpur welcomes Prof. Hawking to IQC on behalf of all Waterloo students and faculty.

Visitors to IQC

HUNDREDS OF DISTINGUISHED GUESTS VISIT IQC EVERY YEAR, FROM LEADING SCIENTIFIC COLLABORATORS TO POLITICIANS, JOURNALISTS, ARTISTS AND MORE. AMONG THEM:

SIR ANTHONY LEGGETT

Winner of the Nobel Prize in Physics in 2003, Leggett is a world-renowned leader in the theory of low-temperature physics. His two-month stay and summer lecture series at IQC have become an annual highlight for faculty and students. He is an Honorary Fellow of the Institute of Physics (U.K), a Mike and Ophelia Lazaridis Fellow, and was knighted (KBE) by Queen Elizabeth II in 2003 "for services to physics."

STEVE MACLEAN

The President of the Canadian Space Agency and the second Canadian in history to perform a spacewalk visited IQC as part of a tour of universities and other academic institutions. Given that he has a PhD in physics with a specialty in laser optics, MacLean came to IQC armed with questions and curiosity about the work being done at the institute.

SACHIN PILOT

India's Minister of State in Communications and Technology visited IQC with a delegation in April 2009 to tour the labs and discuss future technologies with Raymond Laflamme.

ROYDEN RABINOWITCH

An internationally acclaimed artist, Rabinowitch delivered a public lecture at IQC in March 2009, in which he discussed humanity's "crisis of being" caused by the scientific revolution. Rabinowitch is the creator of the "Bell for Kepler," a steel sculpture that was displayed at IQC until May 2009, at which time it was relocated to its permanent home in the Waterloo Civic Square.

ROBYN WILLIAMS

Australia's most prominent science broadcaster visited IQC during a nasty winter storm in early 2010. He took the frigid weather in stride, sitting down with Raymond Laflamme for a long interview about quantum information research, which later aired on his popular radio program, *The Science Show*. A veteran of radio and television, Williams has appeared on *Dr. Who* and *Monty Python's Flying Circus*. ■

From **Waterloo** to the **World**

IQC IS HOME TO A RANGE OF EXPERIMENTAL AND THEORETICAL RESEARCHERS WHO REGULARLY COLLABORATE WITH EACH OTHER AND WITH LEADING SCIENTISTS FROM AROUND THE WORLD.

Collaborations lead to many key breakthroughs and dozens of published papers in academic journals. Networks such as QuantumWorks and CIFAR's Quantum Information Program create bridges between researchers, helping to pave the way for collaborative research. QuantumWorks is an NSERC-funded Innovation Platform that links Canadian researchers with industrial and government agency partners to lead Canada into the next technological revolution. CIFAR brings together leading researchers from across Canada and around the world to work collaboratively on advanced research projects. Currently more than 350 researchers are affiliated with CIFAR's 12 research programs.

IQC's collaborators come from institutions in countries such as: **Japan**, **Singapore**, **Austria**, **Australia**, the **United States**, the **United Kingdom**, **France**, **Germany**, **Czech Republic** and **China**. ■

National and International Agreements

IQC has signed six agreements to promote research and exchange of scientists with other organizations.

- **National University of Singapore**
- **IBM**
- **National Science Council of Taiwan**
- **COM DEV**
- **Indian Institute of Technology, Kanpur**
- **National Institute of Informatics, Japan**

Quick Facts

IQC Collaborations 2009/2010

41	Published papers co-authored by IQC faculty and international collaborators
141	External collaborators on publications
6	Grants shared between IQC faculty and non-IQC researchers
46	External collaborators sharing joint grants with IQC faculty members
61	Institutions whose researchers have collaborated with IQC faculty

"Funding QuantumWorks is an important step in having Canada at the leading-edge of science and technology and the impact of quantum technologies cannot be underestimated."

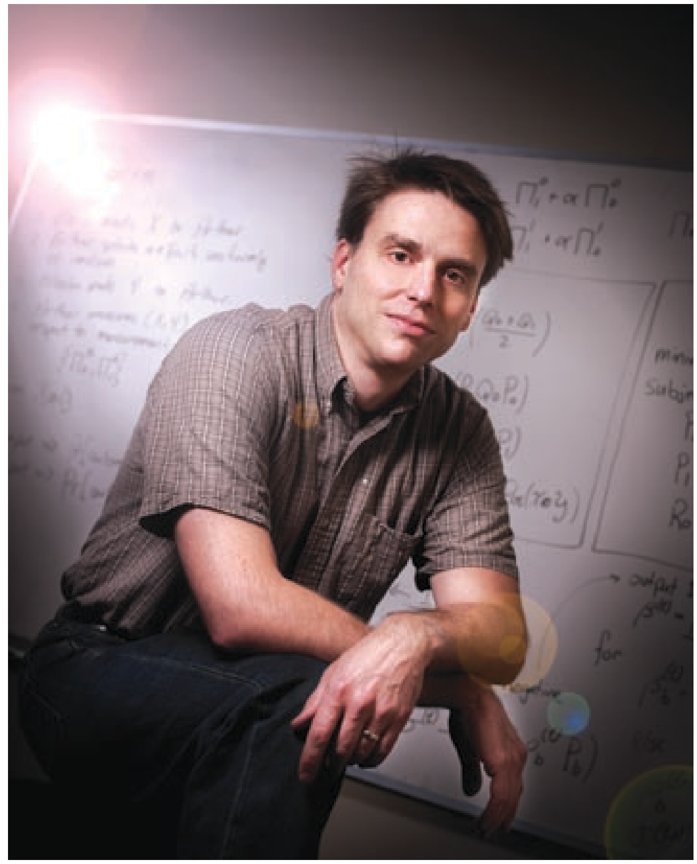
Prof. P. Grutter

Scientific Director, NSERC Nano Innovation Platform

Collaborative Breakthrough

QIP = PSPACE

IQC FACULTY MEMBER JOHN WATROUS AND COLLABORATORS ACHIEVED A MAJOR BREAKTHROUGH IN THE SUMMER OF 2009 WHEN THEY PROVED THE EQUIVALENCE OF TWO COLLECTIONS OF COMPUTATIONAL PROBLEMS CALLED QIP AND PSPACE.



Their landmark discovery was so significant, the paper summarizing their results earned the prestigious Best Paper Award at the Symposium on Theory of Computing (STOC).

The paper, called QIP = PSPACE, was chosen from a field of 279 submissions as having made the most significant contribution to theoretical computer science over the past year.

The discovery resolved a decade-old problem in the theory of quantum computing by proving the equivalence of two collections of computational problems called QIP and PSPACE.

Watrous and collaborators Zhengfeng Ji (Perimeter Institute), Sarvagya Upadhyay (IQC and David R. Cheriton School of Computer Science) and Rahul Jain (National University of Singapore) demonstrated that QIP is equivalent to PSPACE.

To understand the importance of their result, it is helpful to summarize some historical developments that pre-date quantum computing:

PSPACE ("polynomial space") is the collection of all computational problems that can be solved by a computer whose memory usage scales according to some fixed power of the instance size. IP ("interactive proof") designates the class of all computational problems whose solutions can be "verified" through an interaction with a "prover" agent that answers a series of challenge questions, in time bounded by a fixed power of the instance size.

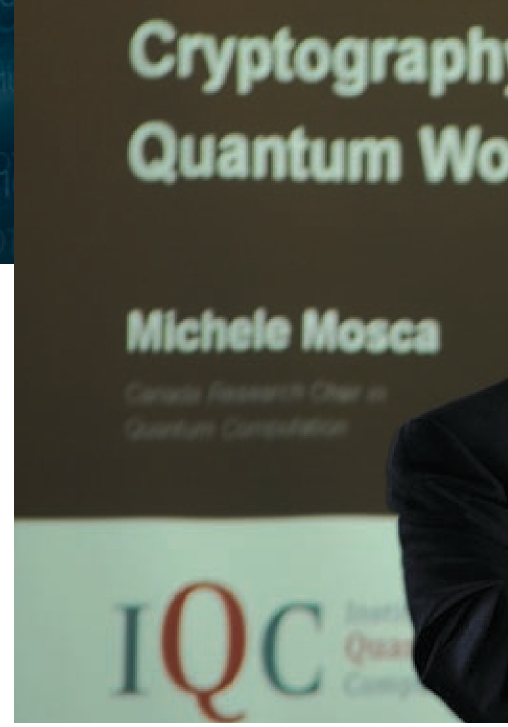
A celebrated result of 20 years ago asserts that IP and PSPACE are in fact two descriptions of the same entity (any problem in PSPACE is in IP, and vice versa).

Watrous was among the first researchers to investigate the quantum analogue of IP, namely QIP. Although he and his collaborators uncovered several interesting properties of QIP, its true relationship to PSPACE remained a mystery until Jain, Ji, Upadhyay and Watrous demonstrated their equivalence last summer.

Explained Watrous: "We want to understand the impact of quantum information on the way we classify the inherent difficulty of computational problems. In the case of interactive proof systems, we now have an answer: quantum information doesn't actually have any effect at all on the class of problems they define."

IQC strives to facilitate such discoveries by creating a fertile environment for collaboration and discovery. ■

Outreach



> “The nineteenth century was known as the machine age, the twentieth century will go down in history as the information age. I believe the twenty-first century will be the quantum age.”

Paul Davies
Physics Professor, Arizona State University

Workshops & Conferences

IQC frequently welcomes many of the top scientific minds in the world to attend conferences and workshops at the institute. From a summer workshop in quantum cryptography for exceptional teenagers to a spintronics conference jointly presented with MIT, these events are designed to spark new ideas, forge new partnerships and build an international community of leading researchers.

The Fourth Workshop on Theory of Quantum Computation, Communication and Cryptography

More than 100 international participants shared recent developments and jointly discussed the latest problems and strategies in quantum information research. Participants visited IQC from Africa, Asia, South America, Europe, North America and Australia.

USEQIP: Undergraduate School on Experimental Quantum Information Processing

An intensive, hands-on workshop aimed at giving roughly a dozen exceptional undergraduate students real-world experience in quantum computation laboratories.

QCSYS: Quantum Cryptography School for Young Students

An introductory workshop to key concepts in quantum information processing aimed at high school students aspiring to study quantum science in university.

Mathematics in Experimental Quantum Information Processing Workshop

A gathering of leading experts in mathematical approaches to quantum information processing.

UW/MIT Spintronics Meeting

An exchange of information and ideas related to spin-based approaches to quantum information processing, led jointly by researchers from IQC and MIT.

USEQIP students preparing for their lectures and lab visits

> “The research done at IQC will help Ontario build a strong and prosperous economy — one based on high skills and high standards.”

Dalton McGuinty
Ontario Premier

Prof. Michele Mosca lectures to a group of young students about Quantum Cryptography

Lectures

Sir Anthony Leggett Lecture Series

Winner of the 2003 Nobel Prize for Physics, Tony Leggett, spends a part of each summer at IQC as a visiting scholar and lecturer. His talks cover subjects at the forefront of quantum information science.

Joseph Emerson Public Lecture

Can quantum mechanics get you out of paying a speeding ticket? Well, no. But IQC faculty member Joseph Emerson presented a compelling case during a packed public lecture hosted by Perimeter Institute on March 3, 2010. Emerson jokingly cited the "Heisenberg Uncertainty Principle" — essentially that we can't measure all properties of an object simultaneously — as the reason why a speeding ticket he received could not be valid. Emerson's lecture included clips from the award-winning documentary *The Quantum Tamers*, which he co-wrote.

The Quantum Tamers

IQC Director Raymond Laflamme and Prof. Joseph Emerson, scientific advisor and co-writer respectively, participated in this documentary spearheaded by the Perimeter Institute. *The Quantum Tamers: Revealing Our Weird and Wired Future* explores the quantum technological revolution. The film won the "Prix Audace" award at the Pariscience International Film Festival.

Community Events

IQC Open House

Each year IQC invites the community to visit the institute to learn about quantum information science. Guests visit the labs, meet IQC's researchers and listen to panel discussions and lectures by some of the world's top quantum information scientists. This year's Open House will take place on September 18 as a participating site on Doors Open Waterloo Region. New this year: science show for kids and other hands-on activities.

TEDxWaterloo

IQC Director Raymond Laflamme explored the power of curiosity at the TEDxWaterloo conference in February 2010. TEDx is a locally organized offshoot of the TED (Technology, Entertainment, Design) conferences, which feature interesting and inspiring speakers and have become a viral Internet phenomenon. "Curiosity is a thread that runs through all of us," Laflamme told an audience of roughly 350. "It is the foundation of all scientific endeavours." ■

> "We will also continue to support and encourage private sector research, development and commercialization of new products and innovations through our national science and technology strategy. For example, we will make further investments in Waterloo's Institute for Quantum Computing, an emerging world leader in the areas of computer, engineering, mathematical and physical sciences."
>
> **Stephen Harper**
> *Prime Minister of Canada*

Participants from the 2010 Tropical QKD Workshop

Michele Mosca, 40 Under 40, *Waterloo Region Record*

Awards

STUDENT AWARDS

NSERC Vanier Canada Graduate Scholarship
Deny Hamel
Gina Passante

David R. Cheriton Graduate Scholarship
Sevag Gharibian
Sarvagya Upadhyay
Gus Gutoski

NSERC Alexander Graham Bell Canada Graduate Scholarship — Doctoral
Jonathan Lavoie
Easwar Magesan

NSERC Alexander Graham Bell Canada Graduate Scholarship — Masters
Ben Criger
Evan Meyer-Scott
Pierre-Luc Dallaire-Demers
Deny Hamel
Robin Kothari

NSERC Postgraduate Scholarship — Doctoral
Jamie Smith
Chris Erven
Christopher Ferrie
Jamie Sikora

NSERC Postgraduate Scholarship — Masters Extension
Deny Hamel
Gina Passante
Ryan Morris
Jamie Smith

Ontario Graduate Scholarship
Thomas McConkey
Kurt Schreiter
Hamid Mohebbi
Brendan Osberg
Jamie Sikora
Cozmin Ududec

Ontario Graduate Scholarship in Science and Technology
Felix Motzoi

President's Graduate Scholarship
Chris Erven
Christopher Ferrie
Pierre-Luc Dallaire-Demers
Thomas McConkey
Evan Meyer-Scott
Gina Passante
Hamid Mohebbi
Ryan Morris
Brendan Osberg
Jamie Smith
Cozmin Ududec
Ben Criger
Deny Hamel
Easwar Magesan
Robin Kothari
Jonathan Lavoie
Kurt Schreiter
Jamie Sikora

Gordon Bell IQC Achievement Award
Bill Rosgen
Matthew McKague
Pierre-Luc Dallaire-Demers
Evan Meyer-Scott
Jean-Luc Orgiazzi

The Mike and Ophelia Lazaridis Fellowship
Devon Biggerstaff
Behnood Ghamsari
Amin Eftekharian
Iman Marvian
Yingkai Ouyang
Chandrashekar Madaiah
Lana Sheridan
Ansis Rosmanis
Farzad Qassemi

FACULTY AWARDS

40 Under 40, *Waterloo Region Record*
Michele Mosca, February 2010

Prix Audace at Pariscience Film Festival
Raymond Laflamme, senior scientific advisor, *Quantum Tamers*
Joseph Emerson, scientific advisor and co-writer, *Quantum Tamers*

"STOC" Prize for Best Paper 2010
John Watrous, QIP = PSPACE with **Rahul Jain**, **Zhengeng Ji**, and **Sarvagya Upadhyay**

POSTDOCTORAL FELLOW AWARDS

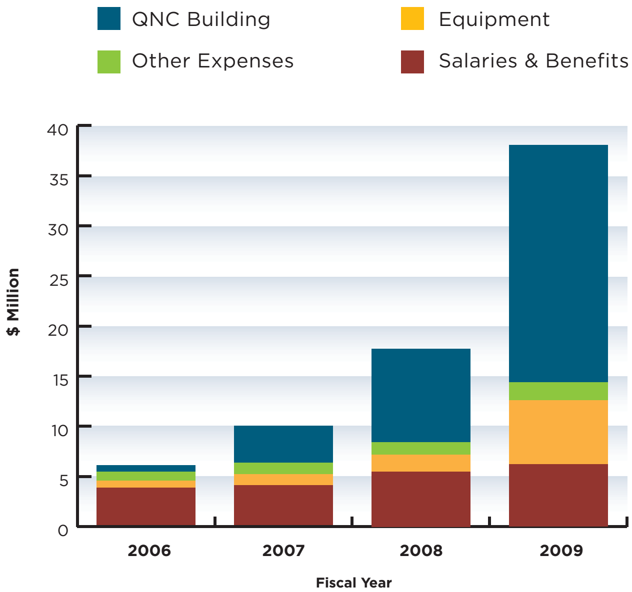
CIFAR Junior Fellow
Jay Gambetta
Bill Coish

NSERC Doctoral Prize
Anne Broadbent

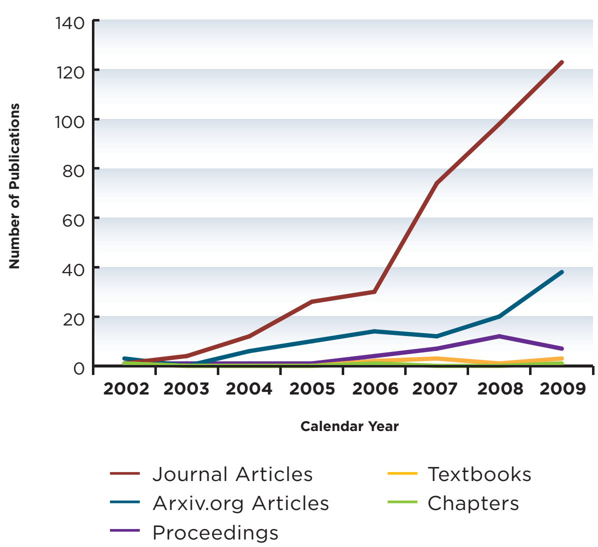
IQC by the NUMB3R5

FISCAL YEAR MAY 1 TO APRIL 30

Annual Expenditures



Publications

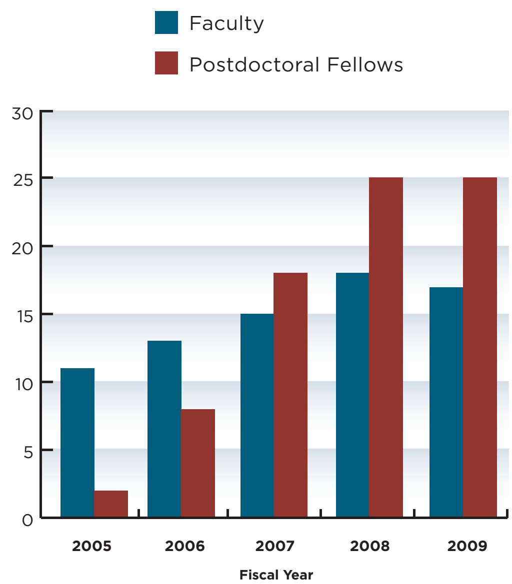


RESEARCHERS AT IQC

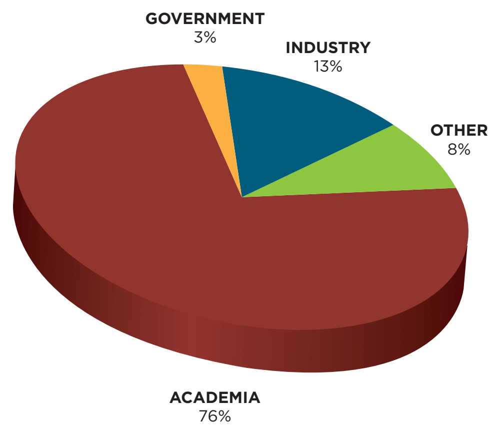
IQC is home to 17 faculty members, 25 postdoctoral fellows, 63 graduate students, two graduate research assistants and 15 undergraduate research assistants.

Faculty & Postdoctoral Fellows

The numbers of faculty members and postdoctoral fellows at IQC have been steadily increasing since inception in 2002.



Graduates in the Workforce



IQC Governance

Board of Directors

Douglas Barber, Distinguished Professor-in-Residence, McMaster University

Tom Brzustowski, RBC Professor, Telfer School of Management, Chair, IQC Board of Directors

Paul Corkum, University of Ottawa and National Research Council

George Dixon, Vice-president, University Research, University of Waterloo

Cosimo Fiorenza, Vice-president and General Counsel, Infinite Potential Group

David Fransen, Consul General, Canadian Consulate General in Los Angeles

Peter Hackett, Executive Professor, School of Business at the University of Alberta & Fellow, National Institute for Nanotechnology

Raymond Laflamme, Director, Institute for Quantum Computing

Mike Lazaridis, President and Co-Chief Executive Officer, Research in Motion

Steve MacDonald, Chief Operating Officer, Institute for Quantum Computing

Michele Mosca, Deputy Director, Institute for Quantum Computing

Peter Nicholson, Retired President, Council of Canadian Academies

William R. Pulleyblank, Professor of Operations Research, United States Military Academy, West Point

Executive Committee

Thomas F. Coleman, Dean, Faculty of Mathematics, University of Waterloo

George Dixon, Vice-president, Chair, University Research, University of Waterloo

Raymond Laflamme, Director, Institute for Quantum Computing

Steve MacDonald, Chief Operating Officer, Institute for Quantum Computing

Terry McMahon, Dean, Faculty of Science, University of Waterloo

Michele Mosca, Deputy Director, Institute for Quantum Computing

Adel S. Sedra, Dean, Faculty of Engineering, University of Waterloo

Scientific Advisory Committee

Harry Buhrman, Professor, Centrum voor Wiskunde en Informatica

Anthony J. Leggett, Professor, University of Illinois at Urbana-Champaign

Gerard Milburn, Professor, University of Queensland

Umesh Vazirani, Professor, University of California, Berkeley

Anton Zeilinger, Professor, University of Vienna

Wojciech Hubert Zurek, Laboratory Fellow, Los Alamos National Laboratory

ACADEMIC, BUSINESS AND INDUSTRY VISITORS TO IQC

Mohamed Abutaleb, Massachusetts Institute of Technology
Dorit Aharonov, Hebrew University of Jerusalem
Sergei Ailujko
Don Aldrige, IBM
Andris Ambainis, University of Latvia
Shiva Amiri, British Consulate
Brandon Armstrong, University of California, Santa Barbara
Atul Asthana, Research in Motion
Roman Barankov, Boston University
Howard Barnum, Perimeter Institute
Steven Bennett, McGill University
Miles Blenowe, Dartmouth College
Hendrik Bluhm, Harvard University
Jérôme Bourassa, Université de Sherbrooke
Fernando Brandão, Imperial College
Eric Brown, McMaster University
Todd Brun, University of Southern California
Harry Buhrman, Centrum Wiskunde & Informatica
Daniel Burgarth, Imperial College
Pierre Bury, Research In Motion, France, Government Relations
Renjie Butalid, TEDxWaterloo
Adán Cabello, Universidad de Sevilla
Earl Campbell, University College London
Gregory Chaitin, IBM
Matthew Cheriyan, Industry Canada
Chen-Fu Chiang, University of Central Florida
Cheng Chin, University of Chicago
Jerry Chow, Yale University
Lai Choy Heng, National University of Singapore
Alessandro Cosentino, University of Pisa
Robert Crow, Research in Motion
Toby Cubitt, University of Bristol
Marcos Curty, University of Vigo
Ian D'Souza, COM DEV
Siddhartha Dasgupta, Director, Government Relations, India
Pieter de Groot, Delft University of Technology
Samuel Denny, University of Cambridge
Michel Devoret, Yale University
Dave Dietz, Research in Motion
Artur Ekert, National University of Singapore
Tan Eng Chye, National University of Singapore
Edward Farhi, Massachusetts Institute of Technology
Stephen Fenner, University of South Carolina
Ray Filteau, Carnegie Mellon University
Jan Fischer, University of Basel
Kent Fisher, University of Guelph
Scott Foubister, Thompson Rivers University
André Fougères, National Optics Institute, Quebec
Jonathan Friedman, Amherst College
Chris Fuchs, Perimeter Institute
Dmitry Gavinsky, NEC Laboratories America
Alexei Gilchrist, University of Queensland
Oleg Gittsovich, University of Innsbruck
Frédéric Grosshans, Le Laboratoire de photonique quantique et moléculaire
Otfried Guhne, Institut für Quantenoptik und Quanteninformation
Patryk Gumann, Rutgers University
Aram Harrow, University of Bristol
Avinatan Hassidim, Hebrew University
Jonathan Hodges, Massachusetts Institute of Technology
Catherine Holloway, Dalhousie University
Hideo Hosono, Waterloo Institute for Nanotechnology
Stephen Hughes, Queen's University
Thomas Jochym-O'Connor, McGill University
Olena Juzar
Louis Kauffman, University of Illinois at Chicago
Artem Kaznatcheev, McGill University
Masato Koashi, Osaka University
Richard Kolacz, COM DEV
Piotr Kolenderski, Nicolaus Copernicus University
Alexander Korotkov, University of California, Colorado
Kevin Krsulich, Massachusetts Institute of Technology
Daniel Kumar, University of North Carolina
Anand Kumar, Rochester University
Martin Laforest, Delft University of Technology
Ben Lanyon, University of Queensland
Chris Laumann, Princeton University
Martin Leblanc, Memorial University
Peter Legg, University of Western Ontario
Tony Leggett, University of Illinois at Urbana-Champaign
Konrad Lehnert, JILA/NIST
Yi-Kai Liu, Caltech
Nancy Lu, University of Calgary
Eric Lucero, University of California, Santa Barbara
Jeff Lundeen, National Research Council Canada
Steve MacLean, Canadian Space Agency
Robin MacNab, Foreign Affairs and International Trade
Vladimir Manucharyan, Yale University
David Marcos, The Instituto de Ciencia de Materiales de Madrid
Alberto Marino, University of Rochester
John Martinis, University of California, Santa Barbara
Dmitry Matsukevich, University of Maryland
Helen McDonald, Information Technologies and Telecommunications
Roger Melko, University of Waterloo
Nicolas Menicucci, Perimeter Institute
Spyridon Michalakis, Los Almos National Laboratory
Gerard Milburn, University of Queensland
Morgan Mitchell, The Institute of Photonic Sciences
Rajat Mittal, Rutgers University
Ghadir Mohammadkani, Zanjan University
John Morton, St. John's College, Oxford University
Herve Mouren, Research In Motion France, Government Relations
Ramy Nassar, Research In Motion
Paul Nation, Dartmouth College
Ion Nechita, University of Ottawa
Vincent Nesme, Institut für Theoretische Physik Leibniz Universität Hannover
Katja Nowack, Delft University
Florian Ong, Université de Sherbrooke
Chris Payette, McGill University
Robert Peach, COM DEV
Sachin Pilot, Department of Information Technology, Government of India
Michel Pioro-Ladrière, Université de Sherbrooke
David Poulin, Université de Sherbrooke
John Preskill, Caltech
Giuseppe Prettico, The Institute of Photonic Sciences
Emily Pritchett, University of Georgia
Dave Pryce, RIM France, Government Relations
Dimitry Pushin, Massachusetts Institute of Technology
Jim Rabeau, Macquarie University
Robabeh Rahimi Darabad, Kinki University
Gulshan Rai, India's Department of Information Texhnology
Chandrasekhar Ramanathan, Massachusetts Institute of Technology
Martin Roetteler, NEC Laboratories America
Matthew Rosato, COM DEV
Catherine Rosenberg, University of Waterloo
Mark Rudner, Harvard University
Terry Rudolph, Imperial College
Alex Russell, University of Connecticut
Colm Ryan, Massachusetts Institute of Technology
Mark Saffman, University of Wisconsin
Yuval Sanders, University of Calgary
Miklos Santha, National University of Singapore and Laboratoire de Recherche en Informatique
Preeti Saran, Consul General of India in Toronto
Chelsea Schmaltz, University of Waterloo
Volkher Scholz, Leibniz Universität Hannover
Thomas Schulte-Herbruggen, Technical University Munich
David Schuster, Yale University
Waichi Sekigucki, Nikkei Inc.
Pranab Sen, Tata Institute of Fundamental Research
David Sevigny, Canada's High Commissioner to Singapore
Krister Shalm, University of Toronto
Adi Shamir, Weizmann Institute of Science
Sarah Sheldon, Massachusetts Institute of Technology
Yun-Pil Shim, National Research Council Canada, Institute for Microstructural Sciences
Peter Shor, Massachusetts Institute of Technology
Stephanie Simmons, St. John's College, Oxford
Kuldip Singh, National University of Singapore
Amandeep Singh, Department of Information Technology, Government of India
William Slofstra, UC Berkeley
Graeme Smith, IBM
Patrick Smutek, Plassys
Jason Soo Hoo, Siena College
Douglas Stebila, Queensland University of Technology
Anya Tafliovich, University of Toronto
Alain Tapp, University of Montreal
Myroslaw Tataryn, St. Jerome's University
Barbara Terhal, IBM Watson Research Centre
Stuart Tessmer, Michigan State University
David Touchette, McGill University
Ian Town, University of Canterbury
Roderich Tumulka, Rutgers University
Stephen Turnbull, McGill University
Robert Ulmer, Counsellor, Embassy of Canada in Japan
Lev Vaidman, Tel Aviv University
Maarten Van den Nest, Max Planck Institute of Quantum Optics
Steven Van Enk, University of Oregon
Lieven Vandersypen, Delft University of Technology
Umesh Vazirani, UC Berkeley
Alipasha Vaziri, Howard Hughes Medical Institute
R Venkatesan, Consulate General of India
Dervis Can Vural, University of Illinois at Urbana-Champaign
Ting-An Wang, TECO Canada
Christian Weedbrook, University of Queensland
Stephanie Wehner, Caltech
Andrew White, University of Queensland
Howard Wiseman, Griffith University
Stuart Wolf, University of Virginia
William Wootters, Williams College
Abuzer Yakaryilmaz, Bogazici University
Fei Yan, Massachusetts Institute of Technology
Mao-Chuang Yeh, University of Illinois
Jun Yin, University of Oregon
Jitong Yu, University of Illinois at Urbana-Champaign
Anton Zeilinger, University of Vienna
Shengyu Zhang, The Chinese University of Hong Kong
Jessica Zhang, Carnegie Mellon University

Management & Administration

Executive Director

Raymond Laflamme

Chief Operating Officer

Steve MacDonald

Deputy Director

Michele Mosca

Administration

Andrew Dale, Administrative Assistant

Monica Dey, Graduate Program Coordinator and Recruitment Assistant

Suzette Pearson, Executive Assistant

Wendy Reibel, Administrative Officer

Marta Szepietowski, Administrative Assistant/Receptionist

Finance

Laurie Kitchen, Financial Analyst

Lorna Kropf, Assistant Director of Administration

Mary Lyn Payerl, Administrative/Financial Assistant

Information Technology

Colin Bell, Computing Support Specialist

Matthew Cooper, Client Support Specialist

Steve Weiss, Manager of Information Technology

Communications and Outreach

Jasmine Graham, Communications Specialist

Katharin Harkins, Associate Director of Communications and Outreach

Colin Hunter, Communications Specialist

Martin Laforest, Manager of Scientific Outreach

Kimberly Simmermaker, Event/Visitor Coordinator

Laboratory Support

Michael Ditty, NMR Facility Manager

Brian Goddard, Senior Fabrication Equipment Technologist/Lab Instructor

Vito Logiudice, Director of Operations, Fabrication Facility

life @ IQC

Monday afternoon hockey

Wednesday afternoon basketball

Halloween at IQC

IQC Summer Golf Tournament

IQC Holiday Party

USEQIP students at the Toronto Blue Jays' game

Thank you

In 2009, Industry Canada granted IQC $50 million over a five-year period to enable the establishment of a new world-class research facility. The project will support the Canadian government's science and technology strategy aimed at building a strong economy via knowledge and innovation.

In 2006, the Province of Ontario (through the Ministry of Research and Innovation) granted $50 million to IQC to help strengthen Ontario's leading-edge research capacity. The grant was used partially to fund the construction of the Mike and Ophelia Quantum-Nano Centre.

IQC thanks the Province of Ontario, Industry Canada and Canada's Economic Action Plan for their continued support.

IQC wishes to thank the following individuals and organizations for their generous and continued support:

- Army Research Office
- Bell Family
- Bruker Biospin Canada
- Canada Foundation for Innovation
- Canada Research Chairs
- Canada's Economic Action Plan
- Canadian Institute for Advanced Research
- Canadian Institute for Photonic Innovations
- Centre for Applied Cryptographic Research
- Centre for Quantum Technologies, Singapore
- COM DEV
- Communications Security Establishment Canada
- Defense Advanced Research Projects Agency
- Disruptive Technology Office
- Early Researcher Awards
- European Research Association
- Fields Institute
- France Canada Research
- Government of Canada
- IBM
- Institut de Ciències Fotòniques
- Institute for Computer Research, University of Waterloo
- Intelligence Advanced Research Projects Activity
- Massachusetts Institute of Technology
- Mathematics of Information Technology and Complex Systems
- Mike and Ophelia Lazaridis
- National Science Council of Taiwan
- Natural Science and Engineering Research Council
- Ontario Centre of Excellence
- Ontario Innovation Trust
- Ontario Ministry of Research and Innovation
- Ontario Research Fund
- Perimeter Institute for Theoretical Physics
- Province of Ontario
- QuantumWorks
- Research in Motion
- St. Jerome's University
- The City of Waterloo
- University of Waterloo

IQC Institute *for* Quantum Computing

475 Wes Graham Way

Waterloo, Ontario

Published by IQC Communications & Outreach

Editors: Katharin Harkins & Jasmine Graham

Writers: Colin Hunter & Martin Laforest

FSC placeholder

www.iqc.uwaterloo.ca