For immediate release

Unique quantum research institute approved for Calgary

April 19, 2004 (Calgary, AB) – Calgary will be home to one of the world's elite research institutes exploring unsolved puzzles on the frontiers of quantum information science, Dr Barry Sanders, director of the new Alberta Institute for Quantum Information Science, announced this week.

The university has approved the creation of a unique multidisciplinary institute that will advance the frontiers quantum information science. Only a few quantum institutes of this calibre exist in the world. The new institute will eventually link research in computer science, theoretical and experimental physics, chemistry, mathematics, and electrical engineering.

"The U of C institute will attract and educate highly qualified personnel in a field that has considerable potential," says Dr. Harvey Weingarten, president of the University of Calgary. "We expect it to attract top students and faculty and to generate substantial research funds annually to support its important work."

"We want to establish international leadership in quantum information science research, with Canada and the University of Calgary as front-runners in quantum information science," says Dr Barry Sanders, also an iCORE Professor of quantum information science in the department of physics and astronomy at the University of Calgary. "The institute will take advantage of the U of C's expertise in this new science, and its willingness to innovate in the interstices between traditional disciplines."

"The institute will provide an excellent setting for people from various disciplines associated with quantum information science to freely associate ideas and share expertise," says Dr Richard Cleve, University Professor of Computer Science at the U of C and one of the institute's founders.

Quantum information science has a potentially profound impact on everything from Internet security to e-commerce. The institute will focus primarily on experimental and theoretical research with the aim of developing quantum information science, its applications, and high quality personnel to support the growth of this area. International collaborations with other quantum information researchers will be fostered as well as ongoing education programs for the local, national and international community in this emerging field.

The Institute for Quantum Information Science will be funded by the University of Calgary. Partners in this project include the University of Montreal, McGill University and the University of Waterloo.

-30-

Contact: Dr Barry Sanders, iCORE Professor (403) 210-8462, bsanders@qis.ucalgary.ca
Mary Anne Moser, iCORE Communications (403) 949-3306, moser@icore.ca

Backgrounder

---

1) University of Calgary Quantum Information Science Research Team

Barry Sanders, iCORE Professor in Quantum Information Science
Richard Cleve, University Professor, Computer Science
John Watrous, Canada Research Chair in Quantum Computing
David Feder, University Professor, Physics and Astronomy
David Hobill, University Professor, Physics and Astronomy
Robert Thompson, University Professor, Physics and Astronomy

---

2) Three examples of the paradigm shift that quantum information has introduced by combining computing science and quantum physics:

i) Quantum computation

In computing science, there is a class of problems that are not solvable – not because there is no possible answer, but because there is no computer powerful enough to do the calculation in a single lifetime. Quantum computation research is in the process of developing efficient solutions for problems that have long been believed to be intractable in standard computing. This new ability will render essentially all current public-key cryptographic protocols insecure to attackers with quantum computers.

ii) Quantum cryptography

If a quantum computer is created, capable of the quantum computation described above, then the levels of security that we now have to protect our information on computers will be worthless. It is absolutely essential that quantum cryptography be developed out before quantum computers become a reality. Quantum cryptography is a security system that is guaranteed by the laws of physics, rather than principles of mathematical complexity as in standard cryptography. This area of research is now of considerable industrial and commercial interest.

iii) Quantum communication

The idea of a "broadband" network may change radically with quantum communication. This area of research explores ways or transmitting many more bits that classic computing. Significant savings in communication costs for a number of communication and distributed computation tasks are envisioned.