Workshop on Quantum Computing and Cryptography

At

System Planning Corporation (SPC)
1000 Wilson Boulevard, 30th Floor
USA Today Merrit Building
Arlington (Rosslyn), Virginia 22209
703-351-8200

Friday, November 19, 2004

SPONSORED BY:

Office of External Research
Bureau of Intelligence and Research

Office of Space and Advanced Technology
Bureau of Oceans and International Environmental and Scientific Affairs

---

The curious behavior and unexpected rules of quantum mechanics – a science that Albert Einstein helped to develop but was reluctant to fully believe – are leading to the development of two emerging technologies: Quantum Computing and Quantum Cryptography.

Quantum computing offers revolutionary new possibilities for computation. One area in which a quantum computer will vastly exceed the capabilities of any classical computer is the problem of factoring very large numbers. No efficient classical algorithm presently exists for factoring large numbers. Our current system of public key distribution and cryptography – the system that provides us with secure financial transactions over the Internet, and ensures the privacy of our confidential communications – rests almost entirely on the inherent difficulty of factoring the product of two very large prime numbers. However, the unique ability of a quantum computer to execute innumerable operations in parallel allows it quickly solve factoring problems using an algorithm developed by Dr. Peter Shor of MIT. This capability has been experimentally demonstrated at the IBM Almaden Laboratory when a state of the art 7-bit quantum computer provided the prime factors 3 and 5 given the product 15.

As larger quantum computers are built, our current encryption infrastructure will no longer be sufficient to ensure privacy. Fortunately, as the destruction of our current cryptography system looms on the horizon due to one realization of quantum physics, another realization provides the advent of quantum cryptography, which offers unbreakable encryption – just in the nick of time. It is not actually the cryptographic algorithms that are unique in quantum cryptography, but the way in which the cryptographic keys are distributed. Quantum key distribution allows encryption key material to be transferred between parties in a manner that eliminates the possibility for an eavesdropper to obtain a copy of the key. Consequently, communications properly encrypted using this key material are provably unbreakable.

This workshop will examine the current state of research, future expectations and possible implications of quantum computing, quantum algorithms, and quantum cryptography.

Out of consideration to your fellow conference participants, please turn off all cell phones and pagers. All remarks are off the record and not for attribution.

PRELIMINARY AGENDA

12:30 p.m. **Registration and Coffee**

12:45 p.m. **Opening Remarks**

Dr. Lee Morin
Deputy Assistant Secretary for Science
Bureau of Oceans and International Environmental and Scientific Affairs
U.S. Department of State

1:00 p.m. **Panel Discussion**

***Moderator*: Dr. Lee Morin**

Prof. Peter Shor
Morss Professor of Mathematics
Massachusetts Institute of Technology

Dr. Carl Williams
Chief, Atomic Physics Division
National Institute of Standards and Technology

Dr. Richard Hughes
Fellow, Physics Division
Los Alamos National Lab

5:00 p.m. **Closing Remarks and Adjournment**

PARTICIPANTS

Dr. Lee Morin is the Deputy Assistant Secretary for Health, Space and Science Bureau of Oceans and International Environmental and Scientific Affairs at the U.S. Department of State. In this capacity, he continues his vast array of scientific endeavors, including Space, Environmental and Health Issues. Dr. Morin joined the Department of State's Bureau of Oceans and International Environmental and Scientific Affairs in March 2004. Dr. Morin brings a unique background to the Bureau, having been elected as an astronaut candidate by NASA in April 1996. He reported to the Johnson Space Center in August 1996. After completing two years of training and evaluation, he was qualified for flight assignment as a mission specialist and initially assigned technical duties in the Astronaut Office Computer Support Branch, followed by the Astronaut Office Advanced Vehicles Branch. He was then assigned to ISS training tasks in the Shuttle Operations Branch of the Astronaut Office. Morin served on the EVA crew of STS-110 (2002) and has logged over 259 hours in space, including over 14 EVA hours.

Dr. Carl J. Williams is Chief of the Atomic Physics Division, of the National Institute of Standards and Technology (NIST). He coordinates the NIST Quantum Information Program (http://qubit.nist.gov). His research activities involve ultracold atomic collisions, Bose-Einstein condensation, and quantum information. Dr. Williams received his Ph.D. from the University of Chicago in 1987, joined NIST in 1998, and is a Fellow of the American Physical Society. He is the author of over 70 technical publications and speaker at numerous national and international conferences. He was awarded the Department of Commerce Silver Medal in 2003 for his leadership of the NIST Quantum Information Program.

Dr. Richard J. Hughes is a Laboratory Fellow in the Physics Division at Los Alamos National Laboratory. He is principal investigator of projects in both free-space and optical fiber based quantum key distribution. He became a Fellow of the American Physical Society in 1999. In 2001 he was co-winner of an R&D100 Award for "Free-space quantum cryptography". He chairs the Advanced Research and Development Activity's Quantum Information Science and Technology roadmap (http://qist.lanl.gov). Richard has authored over 120 scientific papers on quantum field theory, the foundations of quantum mechanics, quantum cryptography and quantum computation. In his spare time he enjoys ultramarathon trail running over distances of up to 100 miles.

Prof. Peter Shor was born in 1959 in New York City, and grew up in Washington, D.C. and in the San Francisco Bay area. He received a B.S. in Mathematics from Caltech in 1981 and a Ph.D. in Applied Mathematics from M.I.T. in 1985. After a one-year postdoctoral fellowship at the Mathematical Sciences Research Institute in Berkeley, Shor took a job at AT&T Bell Laboratories. Until 1994, he worked mainly on algorithms for conventional computers (combinatorial algorithms, computational geometry and average-case analysis of algorithms) and also did some research in probability and combinatorics. In 1994, after thinking about the problem on and off for nearly a year, Shor discovered an algorithm for factoring large integers into primes on a (still hypothetical) quantum computer. Since then, he has spent most of his research time investigating quantum computing and quantum information theory. In 2003, Peter returned to M.I.T. as Morss Professor of Applied Mathematics. Shor received the 1998 Nevanlinna Award, 1999 MacArthur Fellowship, 2001 King Faisal Prize and became a member of the National Academy of Sciences in 2002.

Out of consideration to your fellow conference participants, please turn off all cell phones and pagers. All remarks are off the record and not for attribution.

TRAVEL DIRECTIONS TO SPC HEADQUARTERS

SPC Headquarters is located on the top floors of the 31-story USA Today/Gannett Building at 1000 Wilson Boulevard, Arlington, VA 22202. This site is two blocks from the Rosslyn Metro station and within easy commuting distance of downtown Washington, the Pentagon, and other government agencies, and it offers conference facilities with spectacular unobstructed views of the Potomac River and the Washington skyline.

Inside the Building

Attendees arriving by **public transportation**, or walking from Rosslyn hotels, metro station, should enter the complex by the main door at 1100 Wilson Boulevard. This is at the intersection of Wilson and N. Kent Street. Once inside the building, walk straight ahead to the escalators. Take the escalators to the Mall Level. Walk straight ahead past shops and offices and past a bank of elevators on your right. Turn right and take these elevators to the 30th floor.

Those using the **parking garage** at 1000 Wilson Boulevard should take the elevator to the Mall Level. After exiting the elevator, turn right and go to the next elevators, which go to the 30th floor. Parking is $11.00 per day.

Travel Directions

From Reagan National Airport:

1. Follow Crystal City signs to Rt. 1 (Jefferson Davis Highway), turn right.
2. Drive approximately 1 mile and bear left on Rt. 110.
3. Proceed approximately 2 miles and take Wilson Boulevard.
4. Exit (on left) into Rosslyn.
5. SPC is on the left in the first tall, silver building.
6. Proceed to the 30th floor.

From Dulles Airport:

1. Take the Washington Dulles Access Road to I-66 East (approximately 17 miles.
2. Exit from I-66 after approximately 7 miles at the Rosslyn exit (No. 73).
3. Turn right from Lee Highway onto Fort Myer Drive.
4. Turn left on Wilson Boulevard.
5. SPC is on the right in the second tall, silver building.
6. Proceed to the 30th floor.

Using Metro: (Orange and Blue Lines) – this is about a two-block walk.

- Take Metro to the Rosslyn stop.
- Exit and walk right along Fort Myer Drive.
- Turn left on Wilson Boulevard.
- SPC is on the right in the second tall, silver building.
- Proceed to the 30th floor.