LABORATORY FOR COMPUTER SCIENCE

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

PHYSICS OF COMPUTATION SEMINAR

Date: Friday, April 8, 1994
Time: Refreshments at 4:00pm
Talk at **4:15pm**
Place: 6-120

A Provably Unbreakable Quantum Cryptographic Protocol

Claude Crépeau
Laboratoire d'Informatique
École Normale Supérieure

Assume that a party, Alice, has a bit x in mind, to which she would like to demonstrate a commitment to another party, Bob. That is, Alice wishes, through a procedure commit(x), to provide Bob with a piece of evidence that she has a bit x in mind and that she cannot change it. Meanwhile, Bob should not be able to tell from that evidence what x is. At a later time, Alice can reveal, through a procedure unveil(x), the value of x and prove to Bob that the piece of evidence sent earlier really corresponded to that bit.

In this talk, we present a new bit commitment scheme based on quantum physics. The major contribution of this work is to provide the first complete proof that, according to the laws of quantum physics, neither participant in the protocol can cheat, except with arbitrarily small probability. In addition, the new protocol can be implemented with current technology. The talk will also give a general introduction to quantum cryptography and provide up-to-date information on state-of-the-art technology and applications of quantum cryptography.

This is joint work with Gilles Brassard (Université de Montréal), Richard Jozsa (Université de Montréal) and Denis Langlois (Université Paris–Sud).

Host: Norm Margolus

This talk is part of a seminar series on adapting computers and computations to the constraints of, and opportunities afforded by, microphysics; and on the development and application of the physical theory of computation and information. This series is being sponsored by the MIT Information Mechanics Group (Lab for Computer Science), in conjunction with the MIT Physics and Media Group (Media Lab), the MIT Porous Flow Project (Earth, Atmospheric and Planetary Sciences), and the Mathematical Sciences Research Group at Thinking Machines Corporation. If you would like to receive electronic notice of these seminars, send email to "poc@im.lcs.mit.edu."