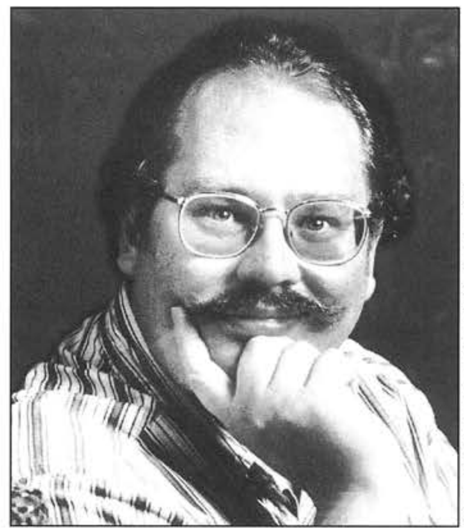
Peter Shor Receives Nevanlinna Prize



Photograph courtesy of the ICM, Berlin, 1998.

Peter Shor

On August 18, 1998, at the Opening Ceremonies of the International Congress of Mathematicians in Berlin Peter W. Shor of AT&T Labs in Florham Park, New Jersey, received the 1998 Rolf Nevanlinna Prize.

The University of Helsinki granted funds to award the Nevanlinna Prize, which honors the work of a young mathematician (less than forty years of age) in the mathematical aspects of information science. The prize is presented every four years in conjunction with the Congress. Previous recipients of the Nevanlinna Prize are Robert Tarjan (1982), Leslie Valiant (1986), Alexander Razborov (1990), and Avi Widgerson (1994).

The committee choosing the 1998 Nevanlinna Prize recipient consisted of Bjorn Engquist (University of California, Los Angeles), Tom Leighton (Massachusetts Institute of Technology), David Mumford (Brown University, chair), and Alexander Razborov (Steklov Mathematical Institute, Moscow).

Peter Shor was born on August 14, 1959. He received his undergraduate degree from the California Institute of Technology and his doctoral degree from the Massachusetts Institute of Technology. Before going to AT&T in 1986 he held a postdoctoral position at the Mathematical Sciences Research Institute in Berkeley.

All present-day computers are based on the laws of classical physics. In the 1980s Paul Benioff, David Deutsch, and Richard Feynman suggested that one could build a far more powerful computer by exploiting principles of quantum mechanics. In 1994 Shor gave the first example of an explicit algorithm by which a quantum computer could solve efficiently (i.e., in polynomial time) a natural problem that seems hard to solve on a classical computer. He developed a quantum algorithm for factorizing integers; no analogous algorithm is known to exist for traditional computers. Earlier work on algorithms for solving problems on quantum computers dealt with more contrived problems and did not supply such complete results as did Shor's. His work caused great excitement among scientists and mathematicians and also drew wider attention because many cryptosystems are based on the difficulty of factoring numbers on conventional computers. Shor has also done work on quantum error-correcting codes and fault-tolerant quantum computation that addresses some of the main obstructions to making quantum computers a reality. Before his work in quantum computing he produced a number of important results in graph theory and combinatorics.

—*Allyn Jackson*