Quantum Computing

Peter Shor

Quantum computers are hypothetical devices which use the principles of quantum mechanics to perform computations. For some difficult computational problems, including the cryptographically important problems of prime factorization and finding discrete logarithms, the best algorithms known for classical computers are exponentially slower than the algorithms known for quantum computers. Although they have not yet been built, quantum computers do not appear to violate any fundamental principles of physics. I will explain how quantum mechanics provides this extra computational power, and outline the factoring algorithm. One of the main difficulties in building quantum computers is in manipulating coherent quantum states without introducing errors or losing coherence. This problem can be alleviated by the use of quantum error correcting codes; if a quantum computer can be built with only moderately reliable hardware, software can be used to make it extremely reliable. I will briefly discuss these issues.

Address: AT&T Labs, Florham Park, USA
E-mail: shor@research.att.com