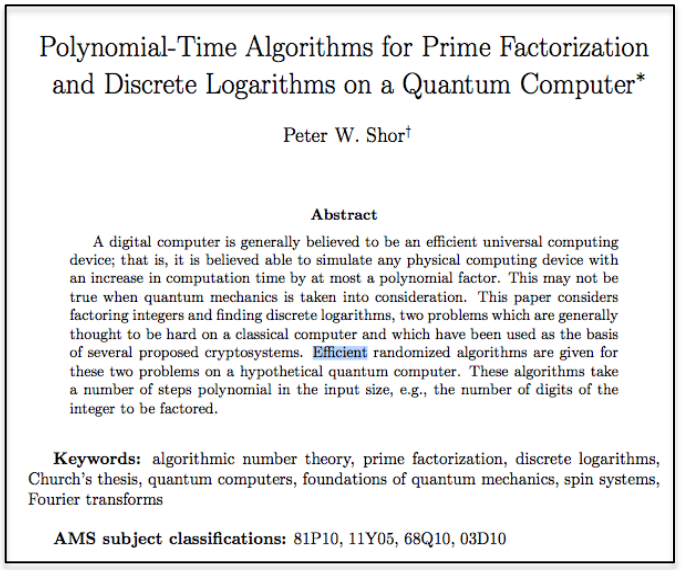
Quantum Information Science

Manipulate and control nature down to the precision of a single quantum.

- **Enabled capabilities**
  - **Quantum computing:** solving currently intractable problems
  - **Quantum communication:** practical ultra-secure communication
  - **Quantum simulation:** developing new classes of materials for new applications
  - **Quantum sensing, metrology and imaging:** sensitivity/precision/resolution beyond best possible with classical means
- **Key research challenges**
  - Maintaining quantum coherence over time
  - Discovering new algorithms that fully exploit QIS for additional new capabilities
  - New techniques to control quantum systems
  - New materials, fabrication for long coherence time



Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

Abstract

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

Keywords: algorithmic number theory, prime factorization, discrete logarithms, Church's thesis, quantum computers, foundations of quantum mechanics, spin systems, Fourier transforms

AMS subject classifications: 81P10, 11Y05, 68Q10, 03D10

Select breakthroughs

- **Quantum factorization algorithm** (Shor 1995): solve intractable problems
- **Quantum gas microscope** (Greiner 2010): observation of an ensemble of atoms in a lattice with down to a single atom resolution