***Shor's Algorithm***

Shor's algorithm is a polynomial-time quantum computer algorithm for integer factorization. Informally, it solves the following problem: Given an integer find its prime factors. It was discovered in 1994 by the American mathematician Peter Shor.

On a quantum computer, to factor an integer , Shor's algorithm runs in polynomial time (the time taken is polynomial in , the size of the integer given as input). Specifically, it takes quantum gates of order using fast multiplication, thus demonstrating that the integer-factorization problem can be efficiently solved on a quantum computer and is consequently in the complexity class BQP. This is almost exponentially faster than the most efficient known classical factoring algorithm, the general number field sieve, which works in sub-exponential time: . The efficiency of Shor's algorithm is due to the efficiency of the quantum Fourier transform, and modular exponentiation by repeated squarings.

If a quantum computer with a sufficient number of qubits could operate without succumbing to quantum noise and other quantum-decoherence phenomena, then Shor's algorithm could be used to break public-key cryptography schemes, such as:

1. The RSA scheme
2. The Finite Field Diffie-Hellman key exchange
3. The Elliptic Curve Diffie-Hellman key exchange

RSA is based on the assumption that factoring large integers is computationally intractable. As far as is known, this assumption is valid for classical (non-quantum) computers; no classical algorithm is known that can factor integers in polynomial time. However, Shor's algorithm shows that factoring integers is efficient on an ideal quantum computer, so it may be feasible to defeat RSA by constructing a large quantum computer. It was also a powerful motivator for the design and construction of quantum computers, and for the study of new quantum-computer algorithms. It has also facilitated research on new cryptosystems that are secure from quantum computers, collectively called post-quantum cryptography.

In 2001, Shor's algorithm was demonstrated by a group at IBM, who factored into , using an NMR implementation of a quantum computer with qubits. After IBM's implementation, two independent groups implemented Shor's algorithm using photonic qubits, emphasizing that multi-qubit entanglement was observed when running the Shor's algorithm circuits. In 2012, the factorization of was performed with solid-state qubits. Also, in 2012, the factorization of was achieved, setting the record for the largest integer factored with Shor's algorithm. In 2019 an attempt was made to factor the number 35 using Shor's algorithm on an IBM Q System One, but the algorithm failed because of accumulating errors. Though larger numbers have been factored by quantum computers using other algorithms, these algorithms are similar to classical brute-force checking of factors, so unlike Shor's algorithm, they are not expected to ever perform better than classical factoring algorithms.