SE 3310b

Theoretical Foundations of Software Engineering

Brief Overview of Quantum Computation and Shor's Algorithm.

Aleksander Essex

Western Engineering

Quantum Speedup

NIST provides a nice list of quantum algorithms and their speedups over classical algorithms. Here are some famous applications:

- **Factoring**: Shor's algorithm for integer factorization provides a super-polynomial speedup over classical algorithms (e.g., General Number Field Sieve). This would break the RSA cryptosystem.
- **Discrete logarithm**: Using a modification to Shor's algorithm, the discrete logarithm problem would similarly be solvable with a super-polynomial speedup. This would break elliptic curve cryptography.
- **Searching**: Grover's algorithm for searching an unordered database provides quadratic speedup over classical algorithms, i.e., $O(\sqrt{n})$ vs. $O(n)$.

Western Engineering