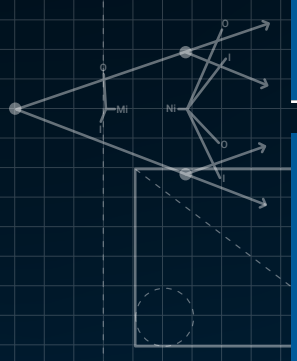
digicert®

- THE SCIENCE
- COMMERCIAL
- GOT/ACADEMIC
- NIST/GOVERANCE

THE HISTORY OF QUANTUM COMPUTING AND PQC



1968 — Stephen Wiesner invents conjugate coding, a basis of the qubit and quantum computing

1980 — Paul Benioff uses Shrödinger's equation to show how a computer could operate on quantum principles

$$i\hbar\frac{\partial}{\partial t}|\psi\rangle=\hat{H}|\psi\rangle$$

1981 — Benioff and Richard Feynman present lectures that push forward a broad interest in the development of quantum, with Feynman focusing on how classical computers can't operate quantum systems

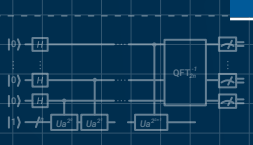
1985 — David Deutsch publishes a description of the universal quantum computer

1988 — Yoshihisa Yamomoto and K. Igeta publish a description of the first physical realization of a photon-based quantum computer, moving the science from the theoretical toward the practical

1994 — Peter Shor publishes "Shor's Algorithm," which allows quantum computers to rapidly factor large integers, the beginning of the science that can break strong classical computing encryption

1996 — Lou Grover publishes an algorithm that can rapidly search databases using quantum computing

Seth Lloyd publishes proof of Feynman's theory about local quantum simulation, meaning a small number of qubits could perform operations that can only possibly be calculated by a vast number of bits in a classical computer



1998 — Isaac L. Chuang at IBM solves Deutsch's problem using a working quantum computer

1999 — Geordie Rose founds D-Wave, the world's first quantum computing company

2000 — Jonathan A. Jones and Michele Mosca at Oxford University solve Deutsch's problem with a working 2-qubit quantum computer

2001 — Shor's algorithm is executed for the first time using a 7-qubit quantum computer developed in partnership between IBM and Stanford University

2007 — Researchers at the Technical University of Munich demonstrate the first 5-qubit quantum computer

2008 — Aram Hassadim, Avinatan Hassadim, and Seth Lloyd publish the Harrow-Hassadim-Lloyd algorithm (HHL) for solving a system of linear equations

2011 — D-Wave demonstrates a 28-qubit quantum annealing computer

2012 — 1QBit is founded as the world's first dedicated quantum computing software company

2016 — D-Wave ONE is announced as the world's first commercially available quantum computer

NIST publishes a report suggesting quantum computers could potentially break the RSA encryption standard by the year 2030, resulting in a call for proposals to build a quantum-safe cryptographic standard

2017 — NIST publishes dozens of PQC proposals and asks for comments

2018 — Google announces the development of a 72-qubit quantum chip IonQ introduces the first commercial trapped-ion quantum computer

2019 — NIST announces PQC set candidates that passed initial testing, seeking comments on the narrowed field for round two

2020 — NIST announces 7 PQC standards finalists and 8 alternatives, seeking comment for round 3

$$i\hbar\frac{\partial}{\partial t}|\psi\rangle=\hat{H}|\psi\rangle$$

Google claims to have achieved quantum supremacy by successfully solving a problem no classical computer could solve in any reasonable amount of time using a superconducting quantum computer

Pan Jianwei and Lu Chaoyang announce The University of Science and Technology of China's Jiuzhang photonic quantum computer has achieved quantum supremacy

2021 — IBM announces the achievement of quantum supremacy

With Jiuzhang 2, Chinese researchers announce they have calculated in 1 millisecond a task that would have taken a classical computer 30 trillion years

2022 — NIST announces the first group of PQC standards that will be recommended for protection against quantum threats: CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, and SPHINCS+

NIST announces candidates for the fourth round of PQC standardization: BIKE, Classic McEliece, HQC, and SIKE

2023 — IBM demonstrates "Condor," an 1121-qubit quantum processor, meeting the company's roadmap goal of breaking the 1,000 qubit threshold

digicert®