Quantum Computing

or, using Schrödinger's cat to solve problems faster

The development of quantum mechanics forced us to drastically rethink the definition of computation, leading to a new computational model called *quantum computing*. This model exploits quantum properties to solve some computational tasks more efficiently, and cryptographic tasks more securely, than classical computers.

TIME LINE

1905 › 35
Development of quantum mechanics

1970
Birth of quantum crypto with Wiesner quantum money scheme

1980 › 90
Theoretical conception of quantum computers

1990 › 2000
Conception of quantum algorithms, error correcting codes, quantum complexity theory

2000 › ...
Boom of quantum computing, first quantum devices

SUBFIELDS

Quantum algorithms. Solving computational tasks related to quantum mechanics (e.g., simulating molecular dynamics), as well as tasks unrelated to quantum mechanics (e.g., factorisation and search)

Quantum cryptography. Using quantum properties to achieve secure protocols for key exchange, money schemes,...

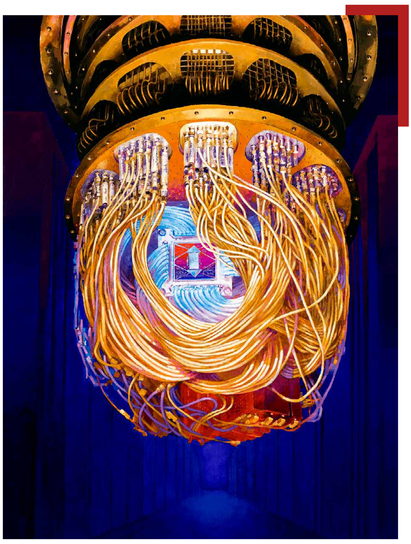
Quantum complexity theory. Fundamental connections between physics problems and quantum complexity classes

Quantum logic and programming languages. Developing and compiling applications on different physical architectures

And more... Quantum information, quantum error correction,...

FROM THEORY TO PRACTICE

In parallel to developing the theory of quantum computation, there is a worldwide effort to actually build quantum computing devices and implement their applications. Some devices are already able to implement certain cryptographic protocols, and even made it to the public market. In contrast, the actual implementation of quantum algorithms is still in its infancy.
Recent years did bring an exciting first step called “quantum advantage”: a quantum device solving a computational task that cannot be efficiently solved by a classical computer.



Google's Sycamore quantum processor used for first quantum advantage experiment