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**

- 1925 - 35: Development of quantum mechanics
- 1970: Wolf of quantum crypto with Wiesner quantum money scheme
- 1980 - 90: Theoretical conception of quantum computers
- 1994 - 2000: Conception of quantum algorithms, error correcting codes, quantum complexity theory
- 2000 - : Boom of quantum computing, first quantum devices

**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.

**Subfields**

- Quantum algorithms: Finding computational tasks related to quantum mechanics (e.g., simulating molecular dynamics, as well as tasks unrelated to quantum mechanics (e.g., factorization and search)
- Quantum cryptography: Using quantum properties to achieve secure protocols for key exchanges, money transfers, etc.
- 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,...

**Protocol for Sharing Secret Key with Perfect Security**

Alice sends state to Bob via untrusted channel.

Using trusted classical channel, Alice and Bob check that Eve did not tamper with the state.