Post-Quantum Cryptography

Cryptographic schemes that can defeat quantum computers

- ➡ Still in research (started around 2006)
- ➡ On August 2024, the NIST released final versions of the first three Post Quantum Crypto Standards

https://en.wikipedia.org/wiki/Post-quantum_cryptography

Quantum Cryptography

The use uses quantum bits and quantum-mechanical phenomena to realize cryptographic tasks

- ➡ Example : Quantum Key Distribution - use a quantum channel to establish a shared key to use on a public channel