WORLD
QUANTUM DAY
APRIL 14

Quantum Computers & Quantum Threat


Esther Hänggi

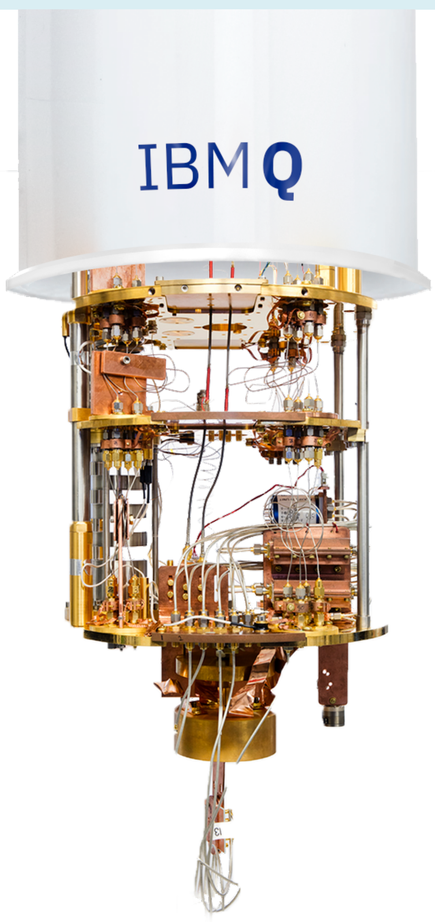

Iyán Méndez Veiga

HSLU Lucerne University of Applied Sciences and Arts

n|w University of Applied Sciences and Arts Northwestern Switzerland


Christoph Wildfeuer


Timeo Jauslin



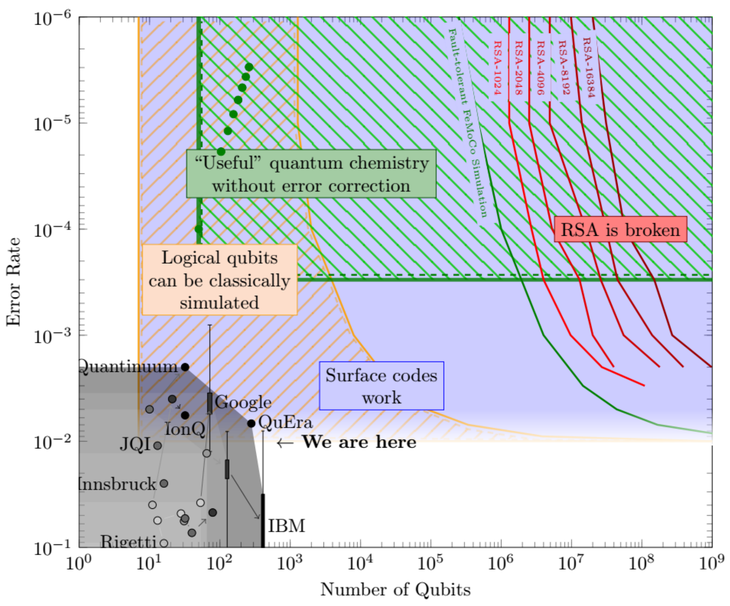
We are still far from having quantum computers that can run Grover's or Shor's algorithms to break current cryptography, but some people think these computeres could be a reality by 2030.

Quantum Computers use quantum bits (or qubits) to perform faster computations

01100101...

Quantum speedup

1110011...



Summary plot by Samuel Jaques (University of Waterloo)

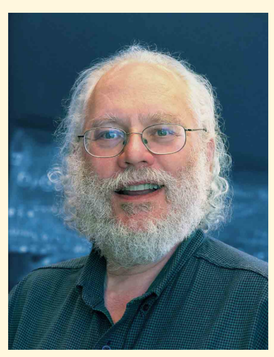
Grover's Algorithm

This quantum algorithm provides a **quadratic speedup** when searching on a unstructured database. It could be use to brute force a 128-bit symmetric cryptographic key in roughly 2^{64} iterations.


Lov Grover

Shor's Algorithm

This quantum algorithm provides an **exponential speedup** to factor numbers and computes discrete logarithms. It could be use to break all current public-key cryptography (RSA, DH, ECC).


Peter Shor

The Quantum Algorithm Zoo

Since the original algorithms by Peter Shor and Lov Grover, many other quantum algorithms have been found with different speedups compared to the best known classical counterparts. A a comprehensive catalog of quantum algorithms can be found here: https://quantumalgorithmzoo.org/

Mosca's law


Michele Mosca