Let's Build a Quantum Computer!

31C3
29/12/2014

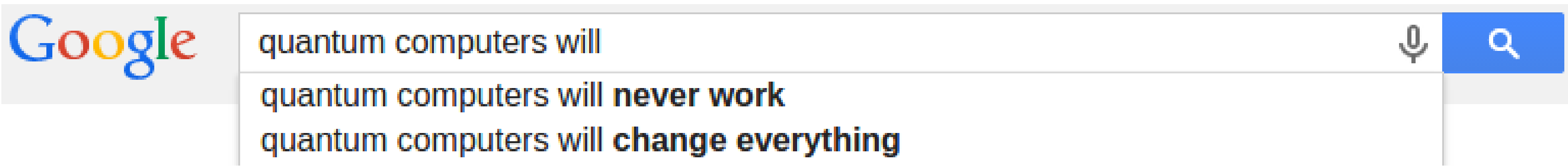
Andreas Dewes

Acknowledgements go to "Quantronics Group", CEA Saclay.

R. Lauro, Y. Kubo, F. Ong, A. Palacios-Laloy, V. Schmitt

PhD Advisors: Denis Vion, Patrice Bertet, Daniel Esteve

Motivation


Google
quantum computers will
quantum computers will **never work**
quantum computers will **change everything**

Outline

Quantum Computing
What is it & why do we want it

Quantum Algorithms
Cracking passwords with quantum computers

Building A Simple Quantum Processor
Superconductors, Resonators, Microwaves

Recent Progress in Quantum Computing
Architectures, Error Correction, Hybrid Systems

Why Quantum Computing?

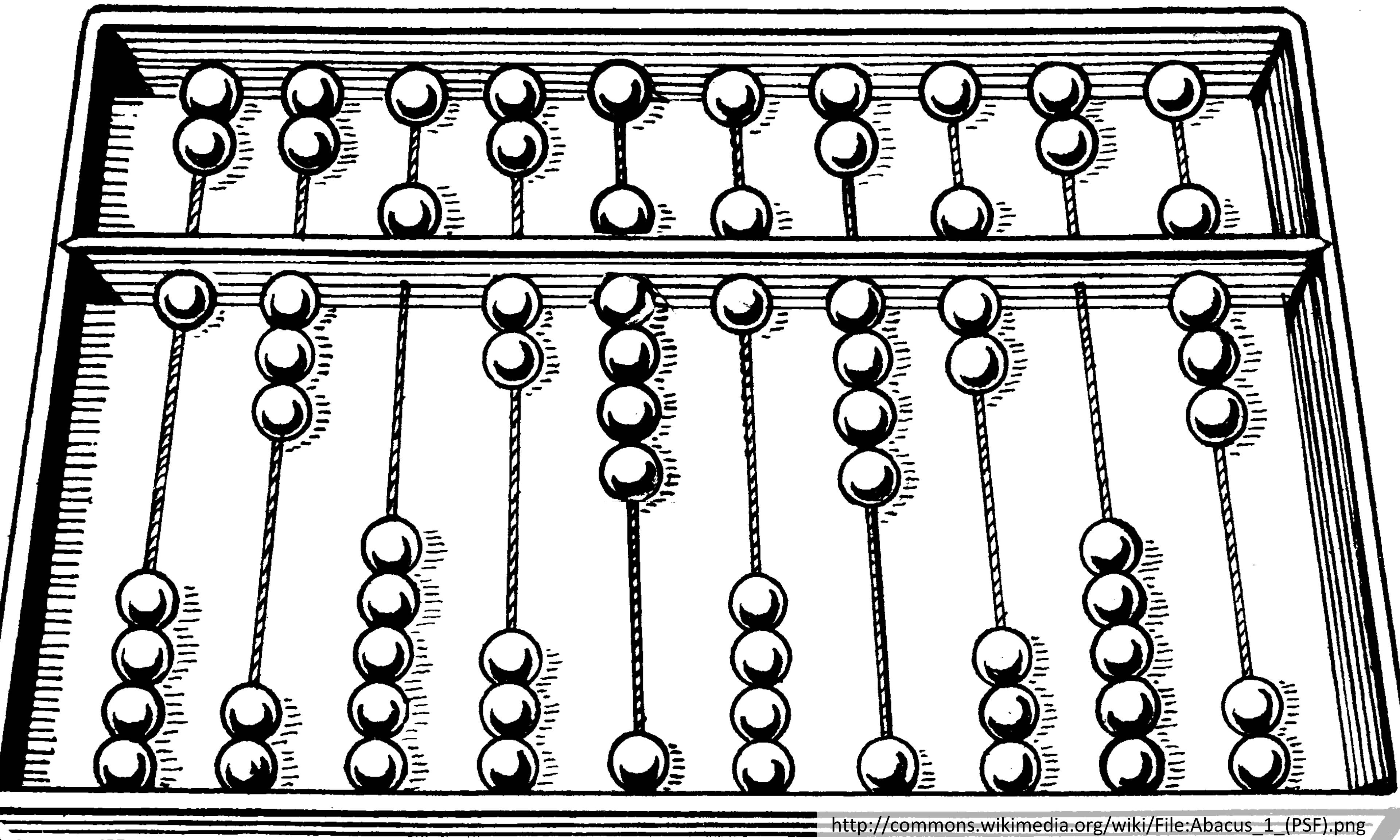
Quantum physics **cannot be simulated efficiently** with a classical computer.[1)]

A computer that **makes use of quantum mechanics** can do it.

It can also be faster for **some** other mathematical problems.

1) http://www.cs.berkeley.edu/~christos/classics/Feynman.pdf

Classical Computing

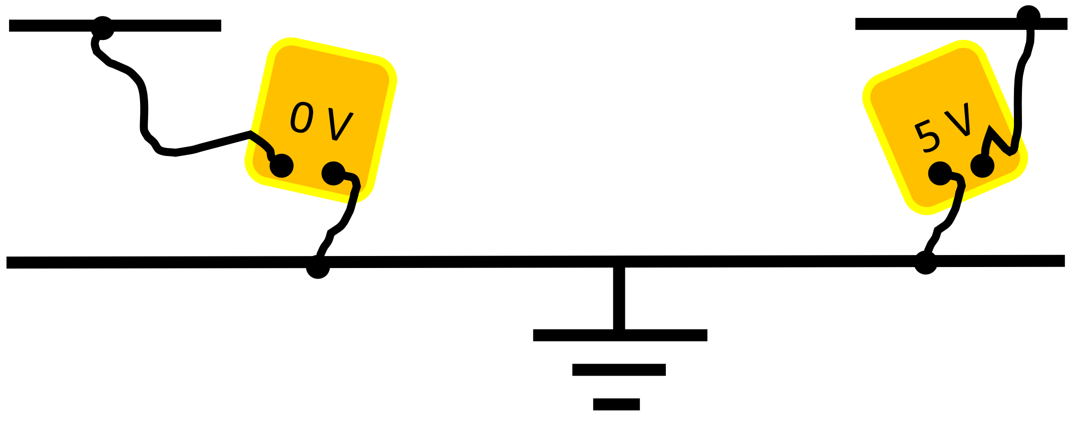


http://commons.wikimedia.org/wiki/File:Abacus_1_(PSF).png

Bits

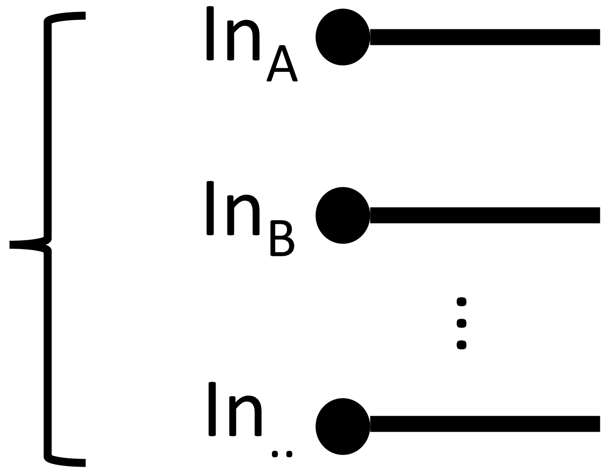
0

1



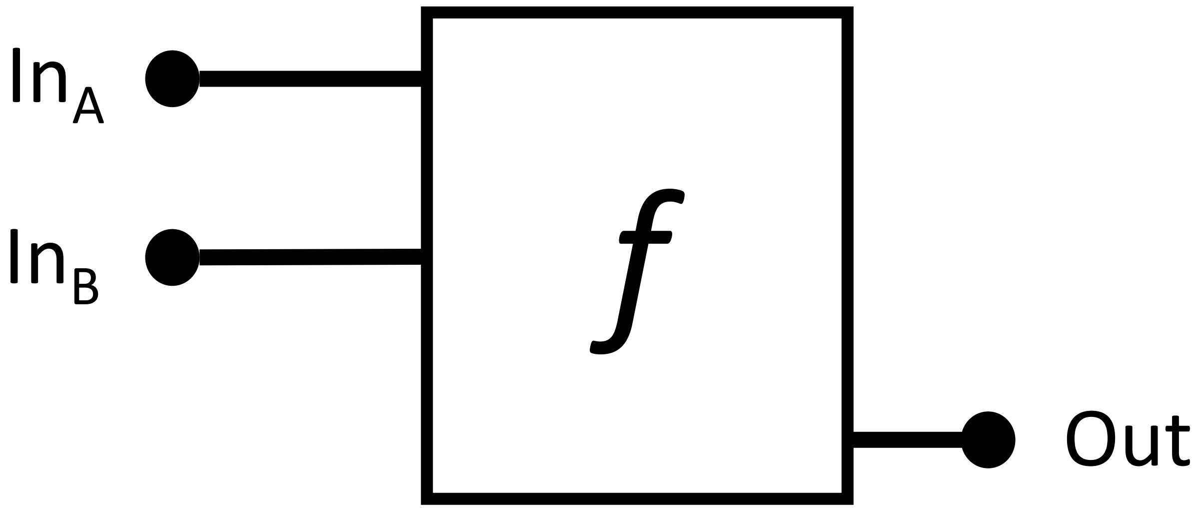
Bit Registers

n bits

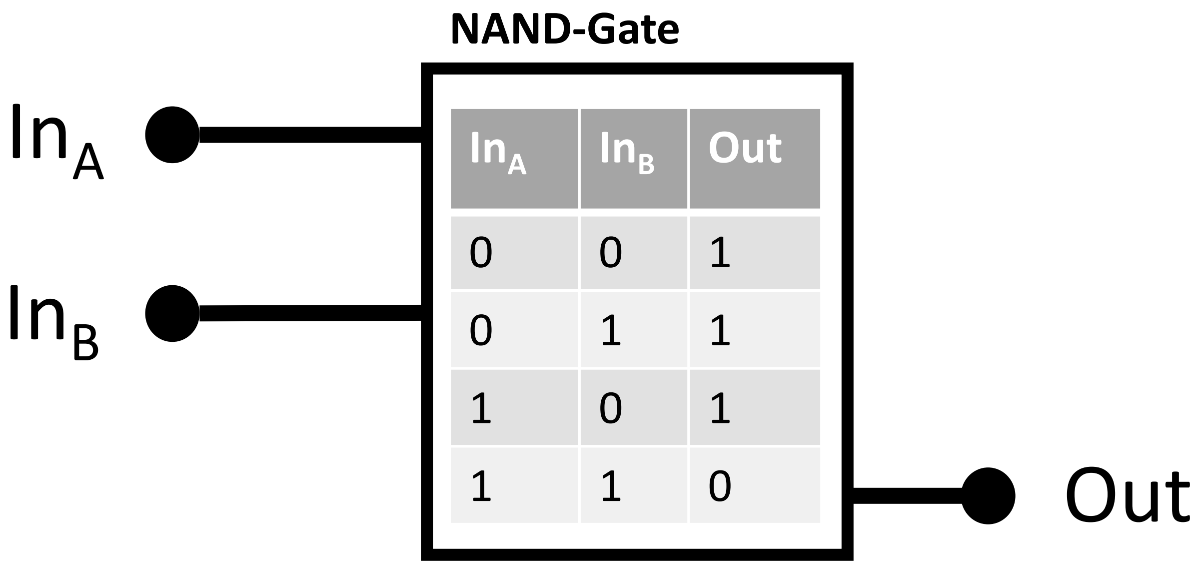


$$\overbrace{0\ldots00, 0\ldots01, \ldots, 1\ldots11}^{N = 2^n \text{ states}}$$

Logic Gates

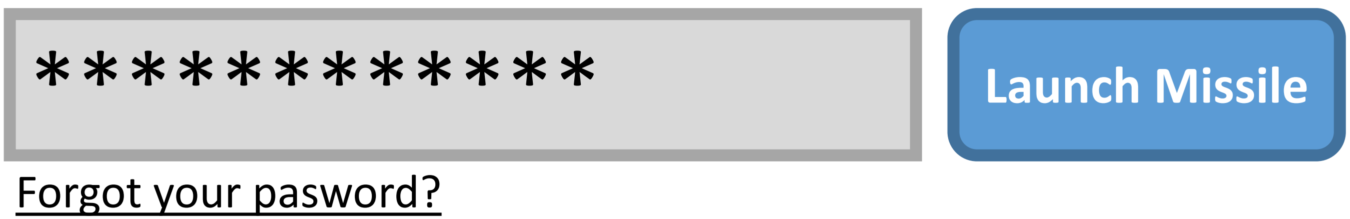


Logic Gates

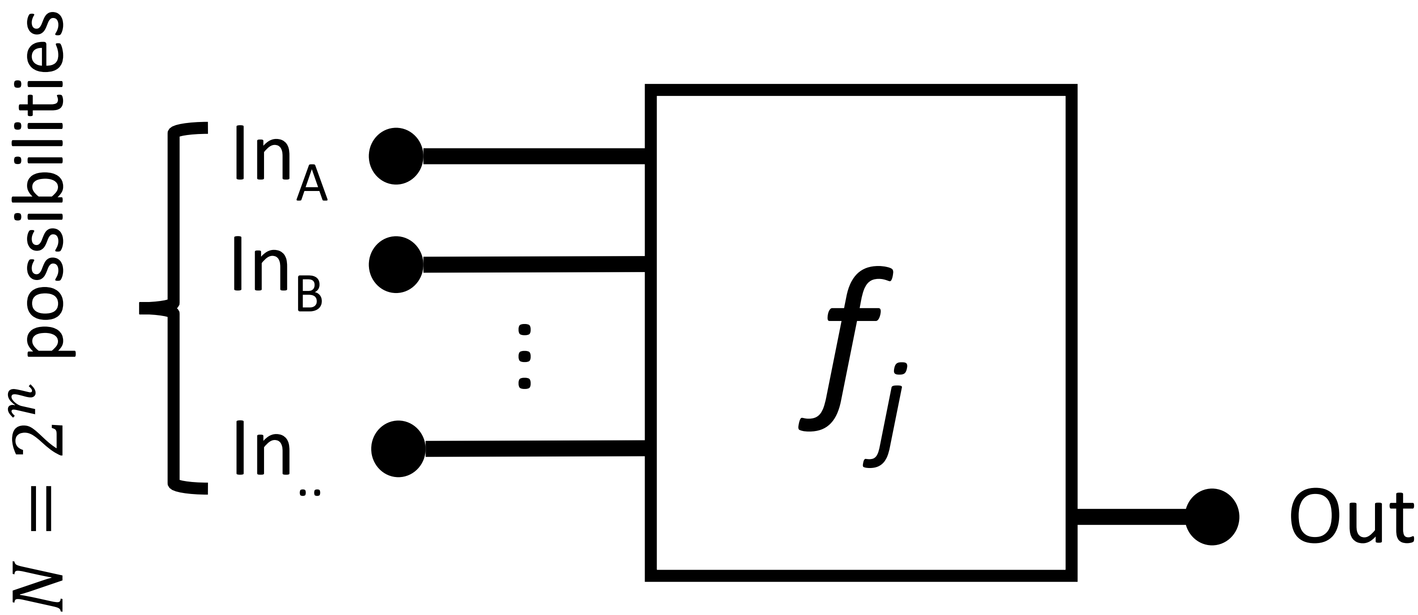


In_A	In_B	Out
0	0	1
0	1	1
1	0	1
1	1	0

A problem: Password cracking



A Password Checking Function



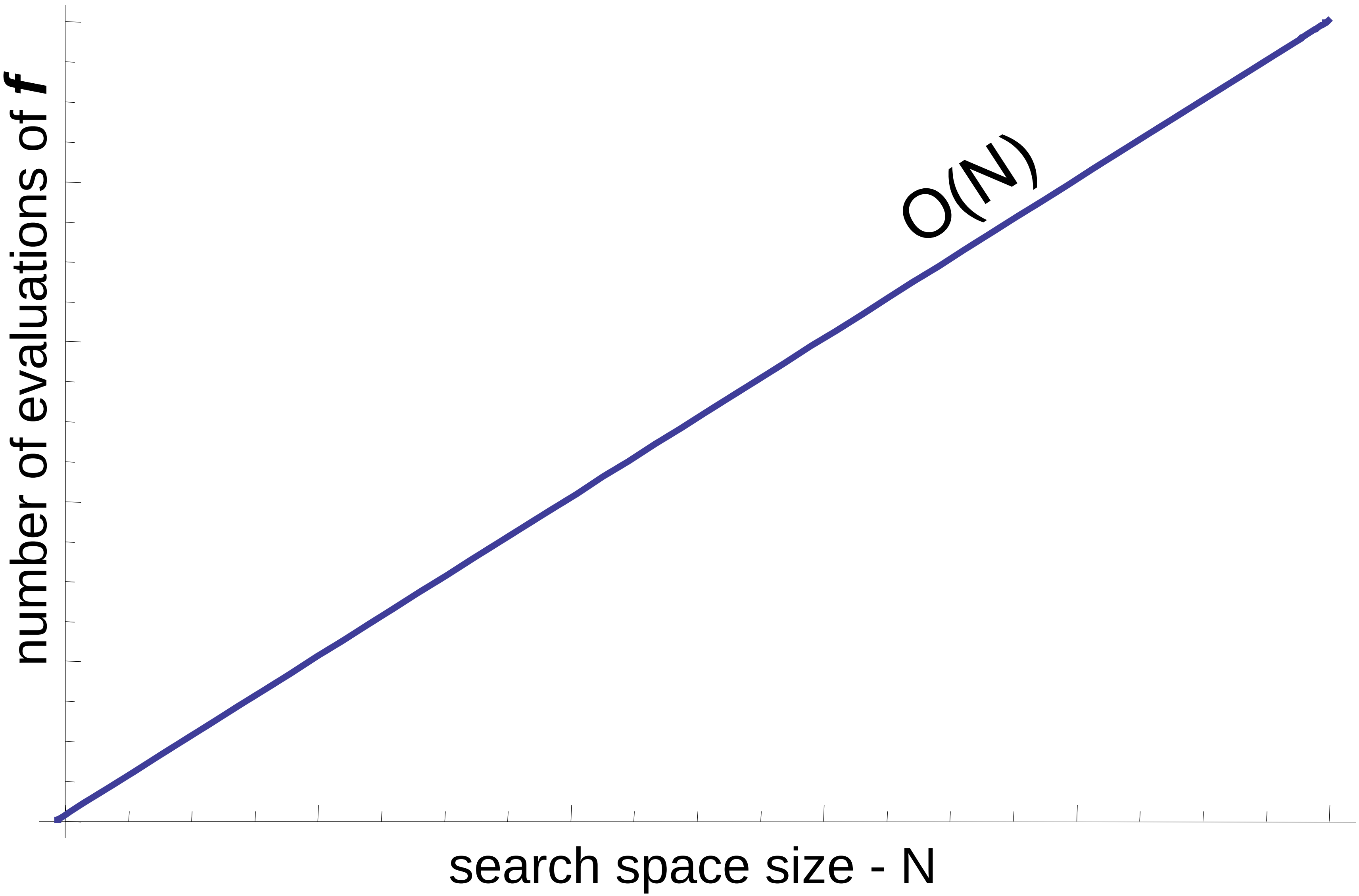
$$f = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases}$$

$$i, j \ \in \{00 \dots 000, 00 \dots 001, \dots, 11 \dots 111\}$$

A Cracking Algorithm

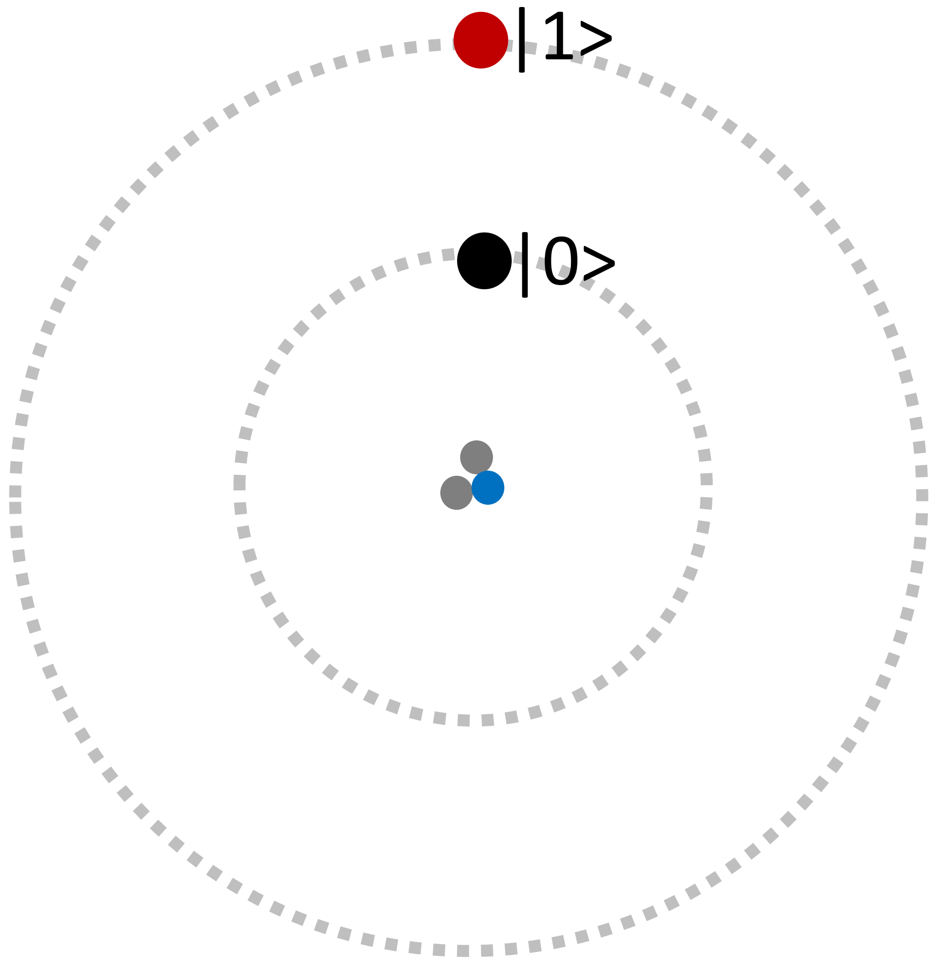
1. Set register state to $\boldsymbol{i} = \mathbf{00000...0}$
2. Calculate $\boldsymbol{f(i)}$
3. If $\boldsymbol{f(i)}= \boldsymbol{1}$, return $\boldsymbol{i}$ as solution
4. If not, increment $\boldsymbol{i}$ by $\boldsymbol{1}$ and go to (2)

Time Complexity of our Algorithm



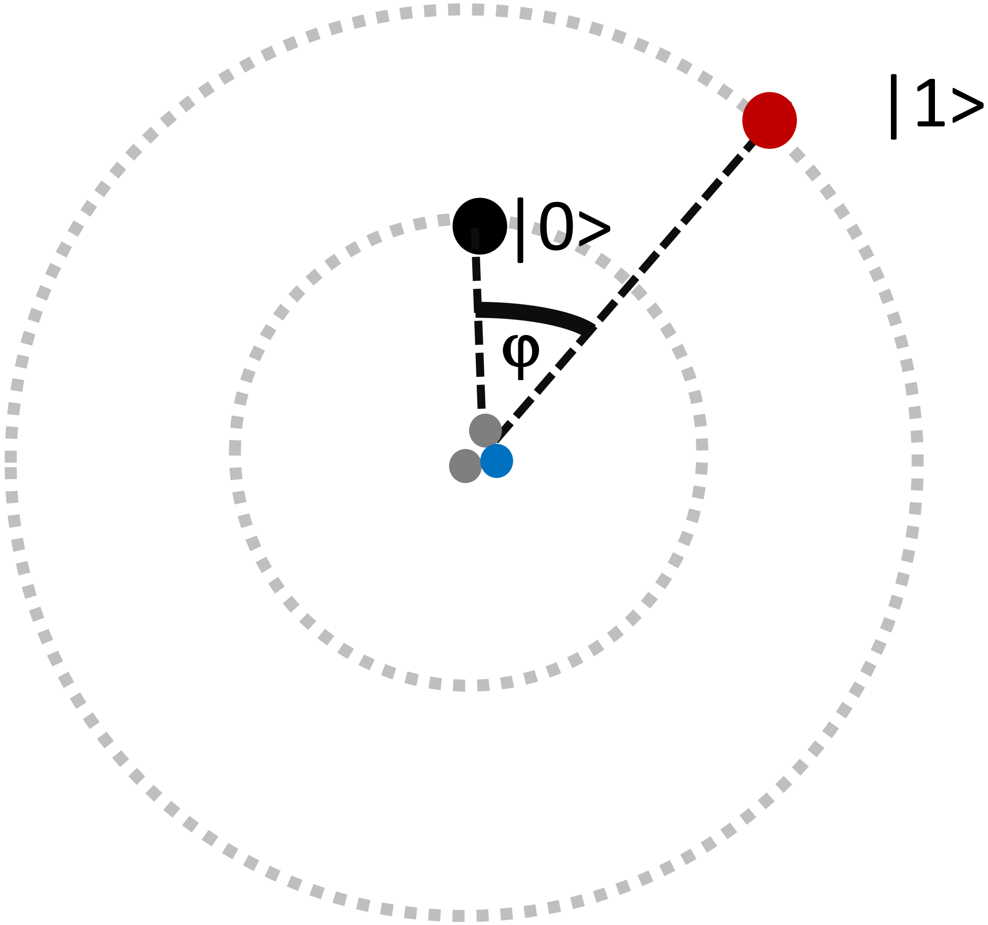
Quantum Computing

Quantum Bit / Qubit



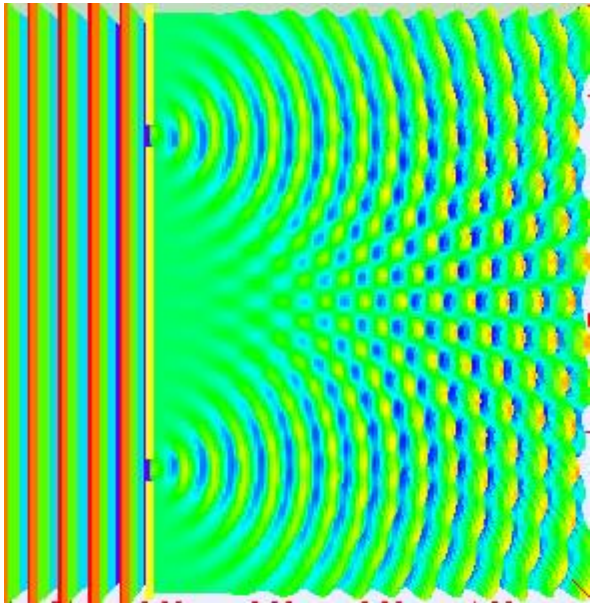
Qubit ≈ **Two-Level Atom**

Quantum Superposition



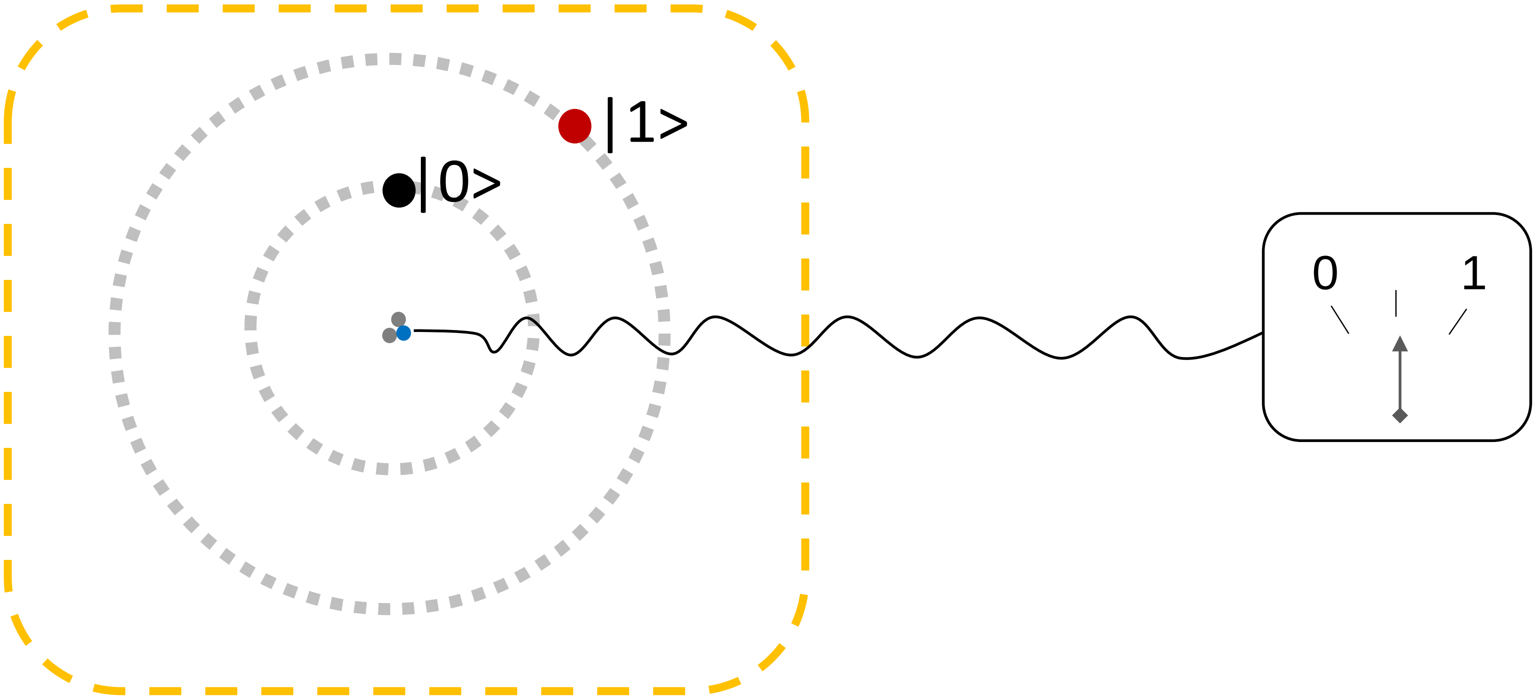
$$|\psi\rangle = \sqrt{a}|0\rangle + \sqrt{1-a} \cdot e^{i\varphi}\,|1\rangle$$

How to imagine superposition



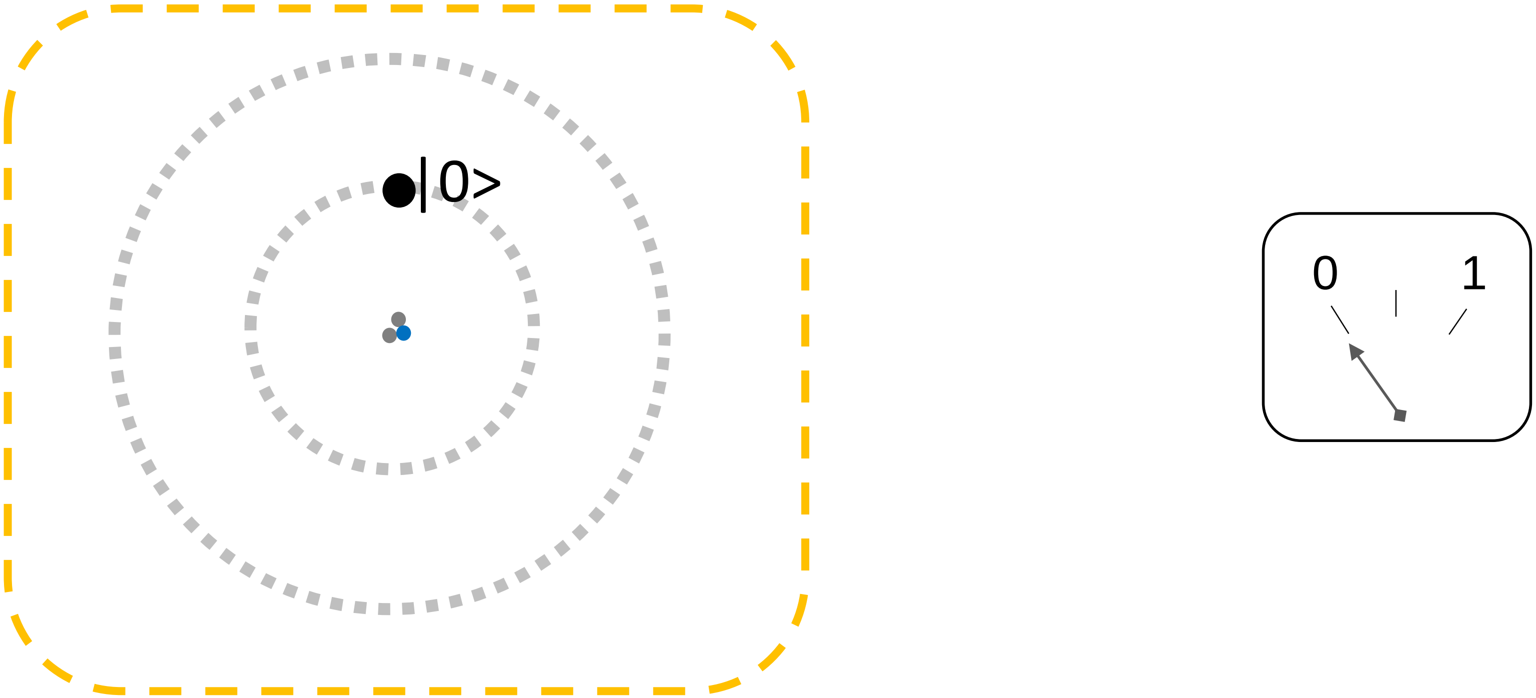
http://en.wikipedia.org/wiki/Double-slit_experiment#mediaviewer/File:Doubleslit3Dspectrum.gif

Quantum Measurements



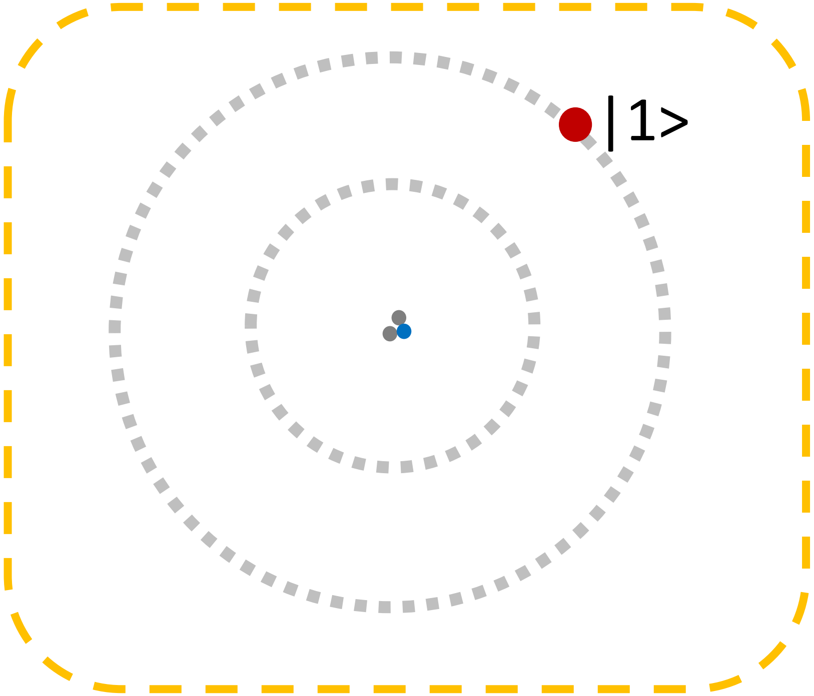
$$|\psi\rangle = \sqrt{a}\,|0\rangle + \sqrt{1-a}\cdot e^{i\varphi}\,|1\rangle$$

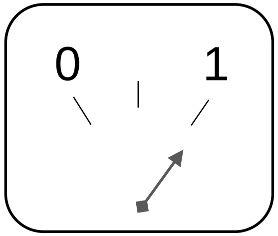
Quantum Measurements



$|\psi\rangle = |0\rangle$; probability = $\boldsymbol{a}$

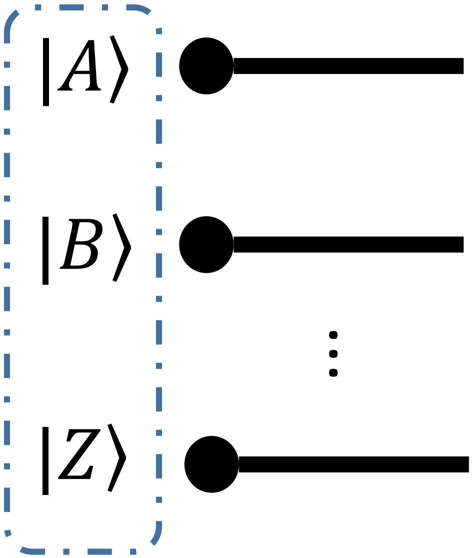
Quantum Measurements





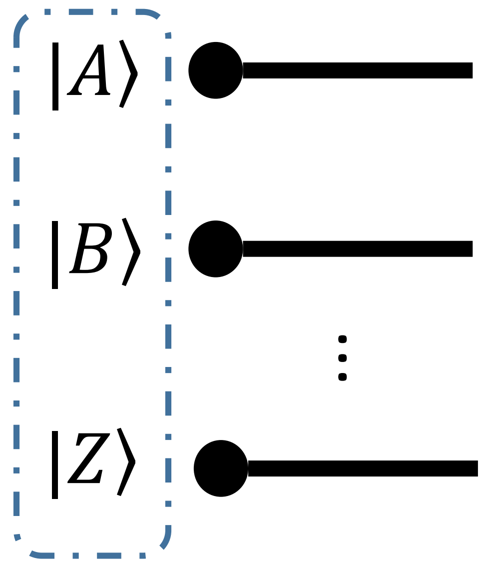
$|\psi\rangle = |1\rangle$; probability = $\boldsymbol{1\text{-}a}$

QuBit Registers



$$|A\rangle|B\rangle\ldots|Z\rangle$$

QuBit Registers



$$\boxed{|AB \ldots Z\rangle}$$

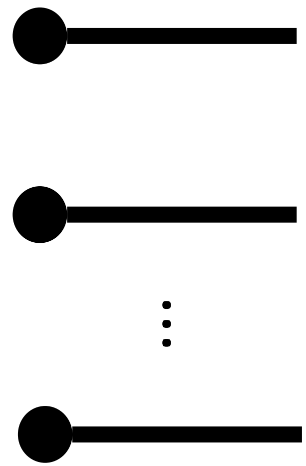
Multi-Qubit Superpositions

$0.5^{1/2}(|0\rangle + |1\rangle)$

$0.5^{1/2}(|0\rangle + |1\rangle)$

$\vdots$

$0.5^{1/2}(|0\rangle + |1\rangle)$



$$0.5^{n/2}\overbrace{(|0\rangle + |1\rangle) \ldots (|0\rangle + |1\rangle)}^{\text{n times}}$$

Multi-Qubit Superpositions

$$0.5^{1/2}(|0\rangle + |1\rangle)$$

$$0.5^{1/2}(|0\rangle + |1\rangle)$$

$$\vdots$$

$$0.5^{1/2}(|0\rangle + |1\rangle)$$

$$0.5^{n/2}(\overbrace{|00 \ldots 0\rangle + \cdots + |11 \ldots 1\rangle}^{N = 2^n \text{ states in superposition}})$$

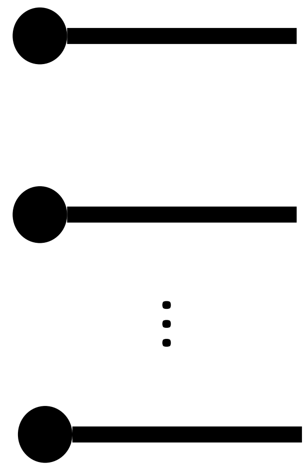
Multi-Qubit Superpositions

omitting normalizations

$$|0\rangle + |1\rangle$$

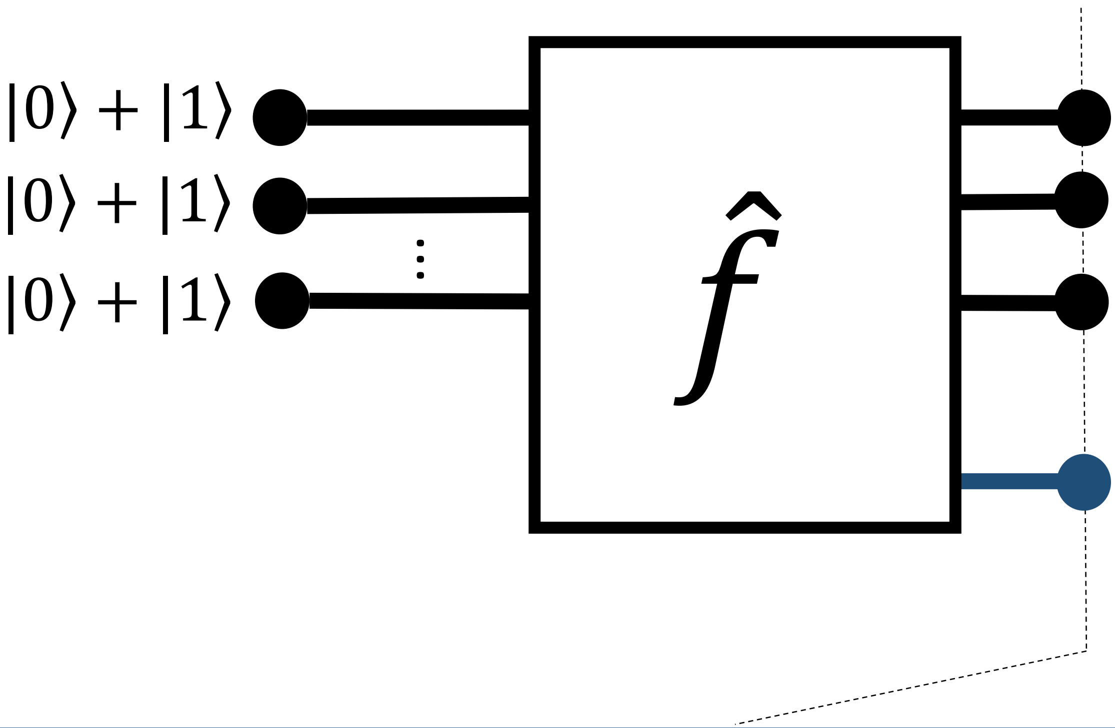
$$|0\rangle + |1\rangle$$

$$|0\rangle + |1\rangle$$



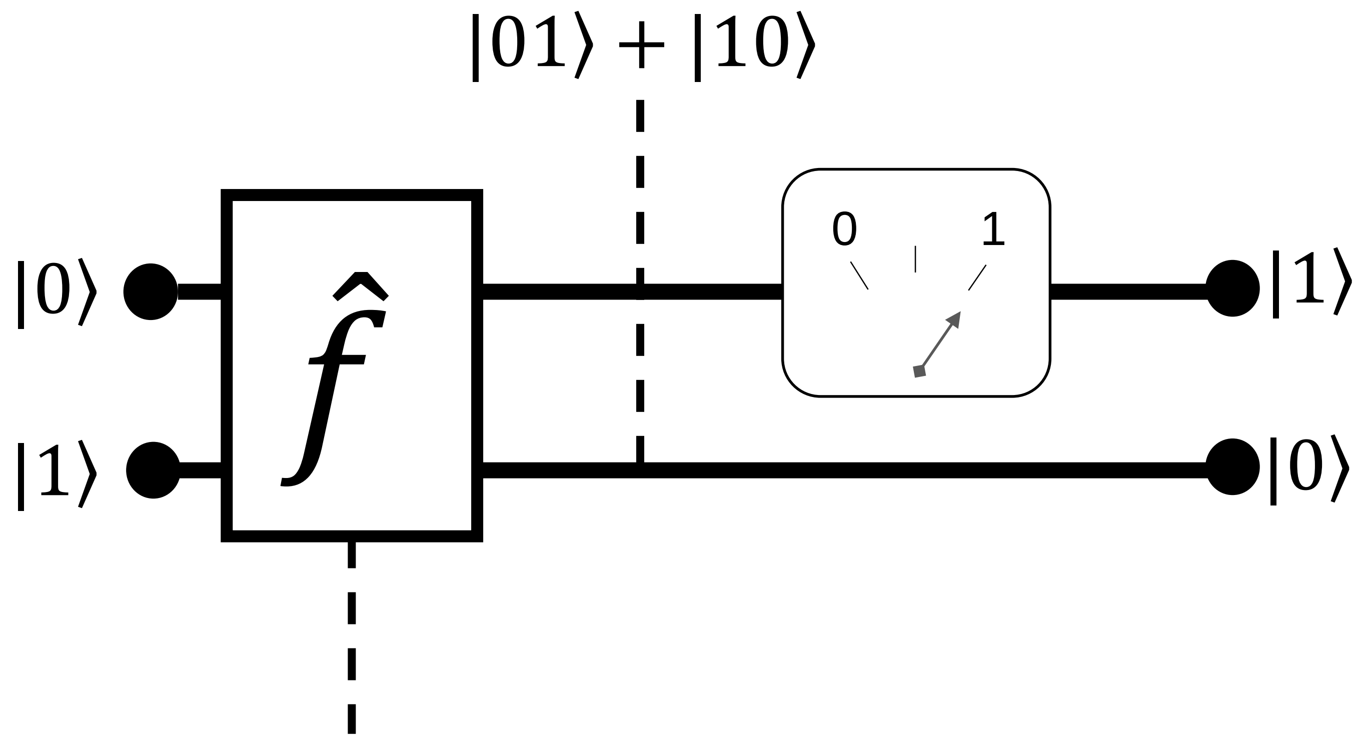
$$|00\ldots0\rangle + \cdots + |11\ldots1\rangle$$

Quantum Gates



$$|0 \ldots 00 \cdot \hat{f}(0 \ldots 00)\rangle + |0 \ldots 01 \cdot \hat{f}(0 \ldots 01)\rangle + \ldots + |1 \ldots 11 \cdot \hat{f}(1 \ldots 11)\rangle$$

Quantum Entanglement



$$\hat{f}(|01\rangle) = |01\rangle + |10\rangle$$

Summary: Qubits

Quantum-mechanical **two-level system**

Can be in a **superposition** state $|\mathbf{0}\rangle + |\mathbf{1}\rangle$

A measurement will yield either $\mathbf{0}$ or $\mathbf{1}$ and **project** the qubit into the respective state

Can become **entangled** with other qubits

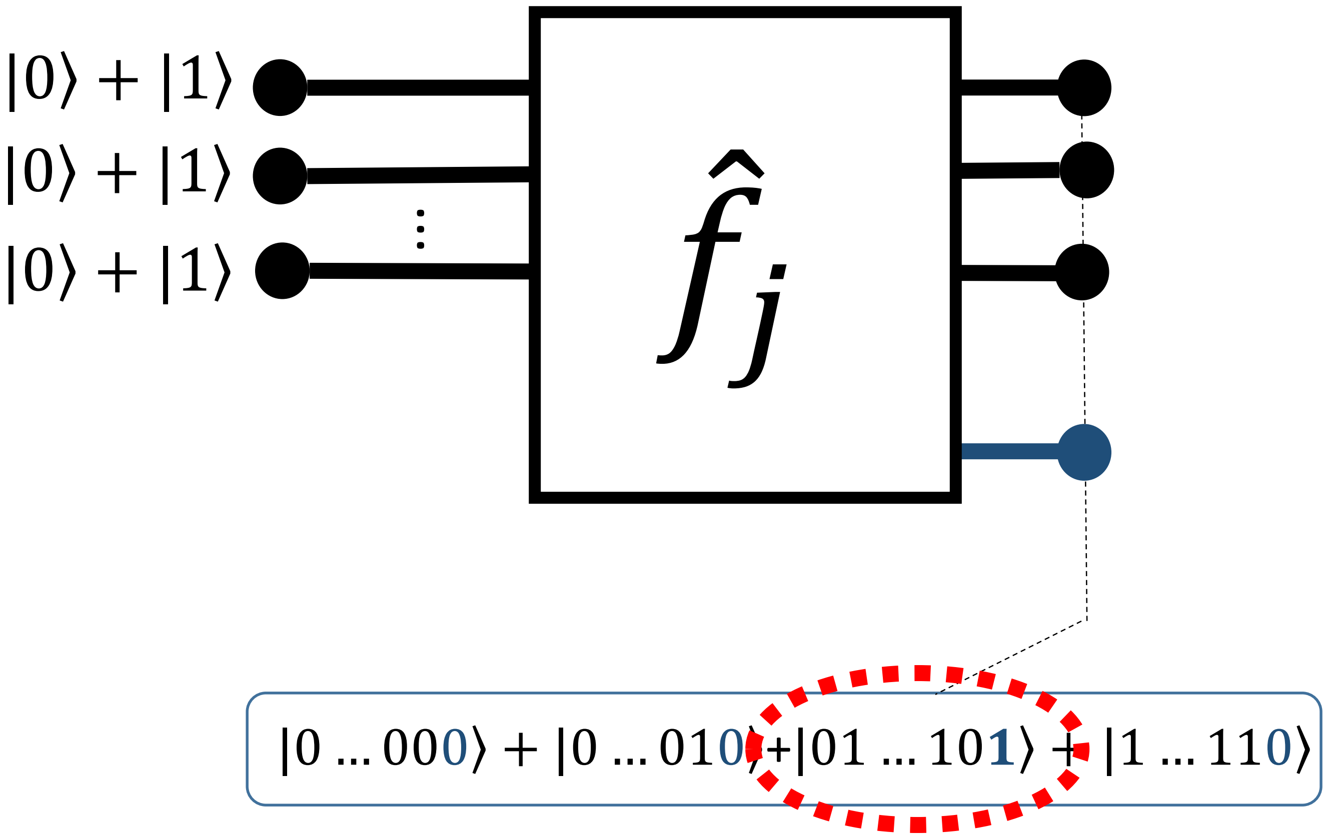
Back to business...

****

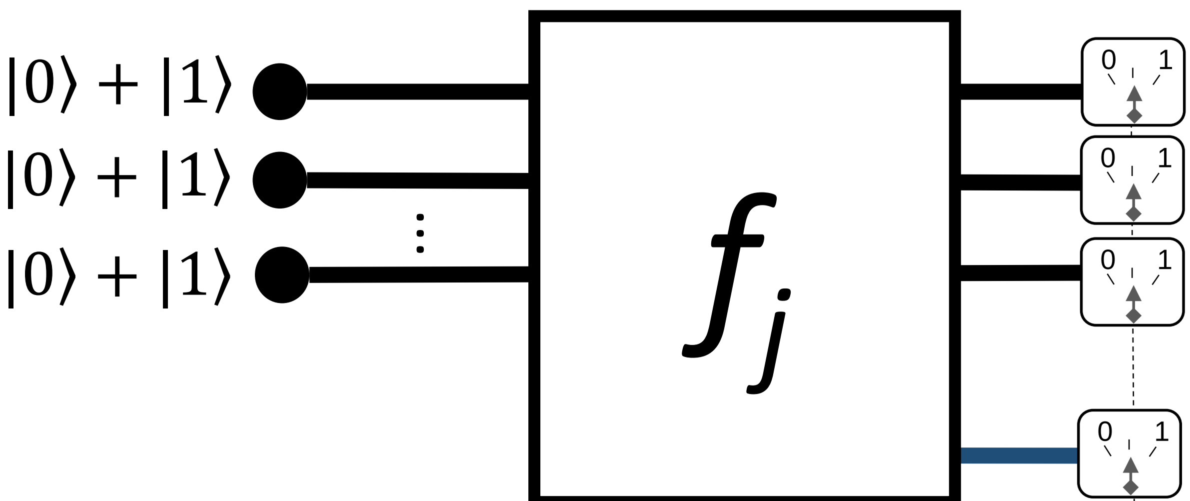
Launch Missile

Wrong password!

Quantum Searching our Password



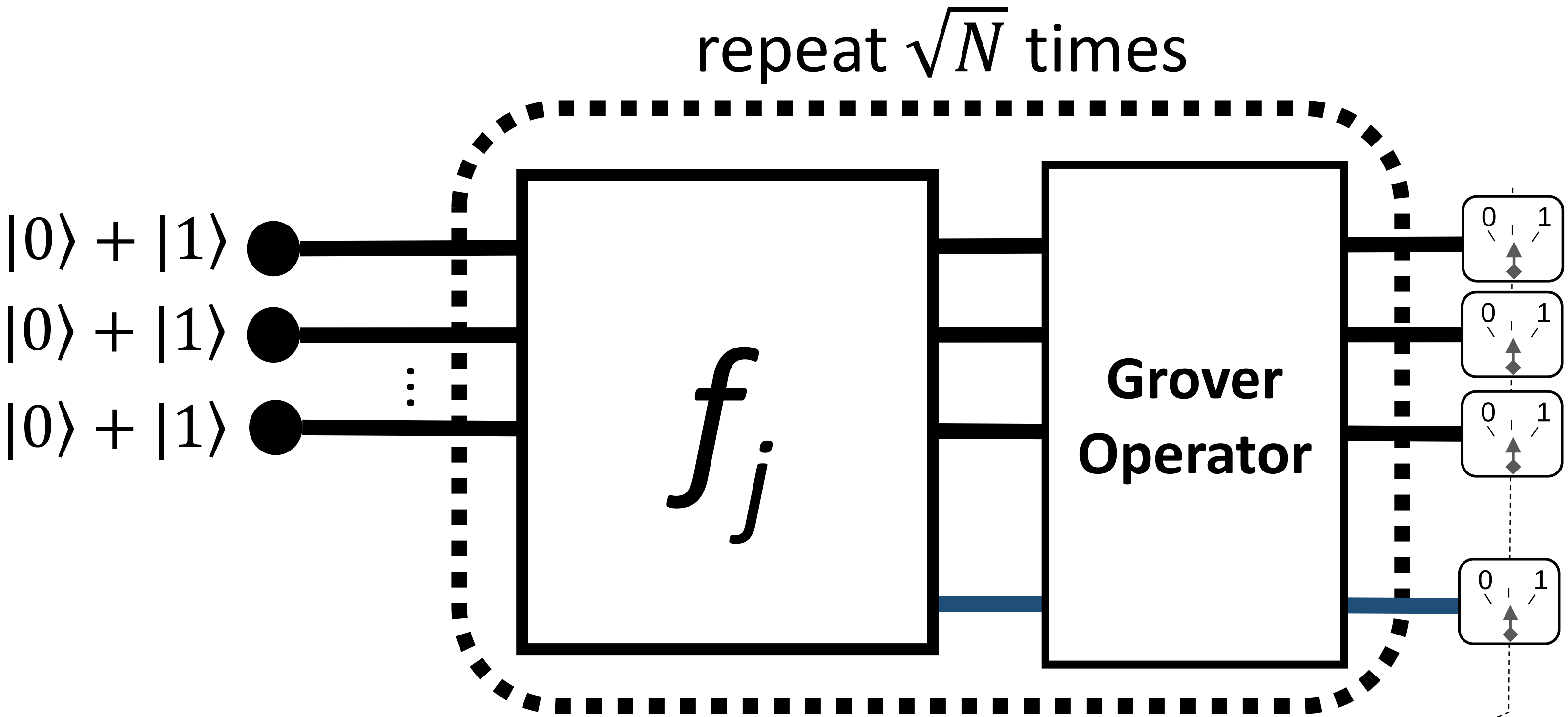
But how we get the solution?



$$result = \begin{cases} 01\ldots10\mathbf{1} & p = \dfrac{1}{N} \\ ** \cdots ** \ \mathbf{0} & p = 1 - \dfrac{1}{N} \end{cases}$$

☹

Solution: Grover Algorithm



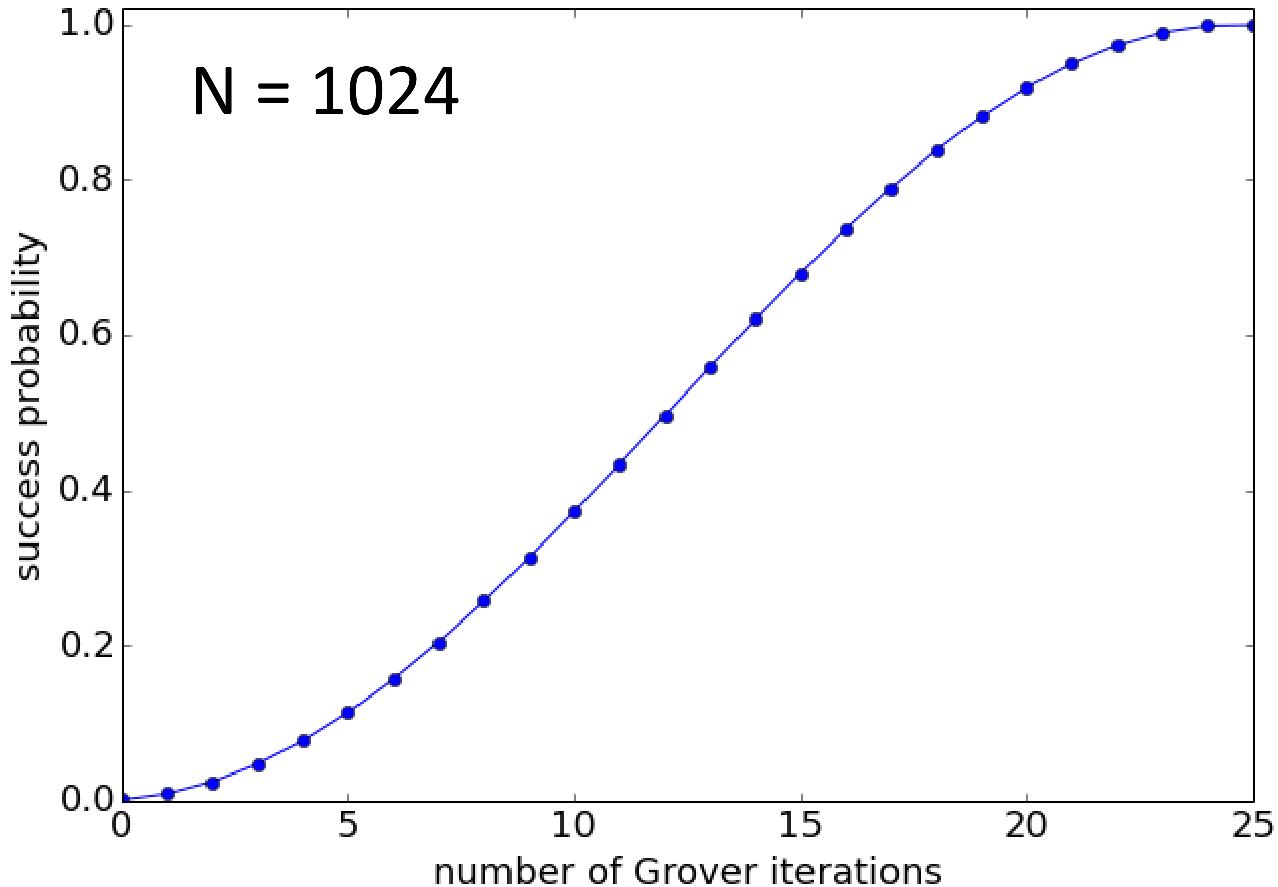
$$result = \begin{cases} 01 \ldots 10\mathbf{1} & p \approx 1 \\ ** \cdots ** \ \mathbf{0} & p \approx 0 \end{cases}$$

☺

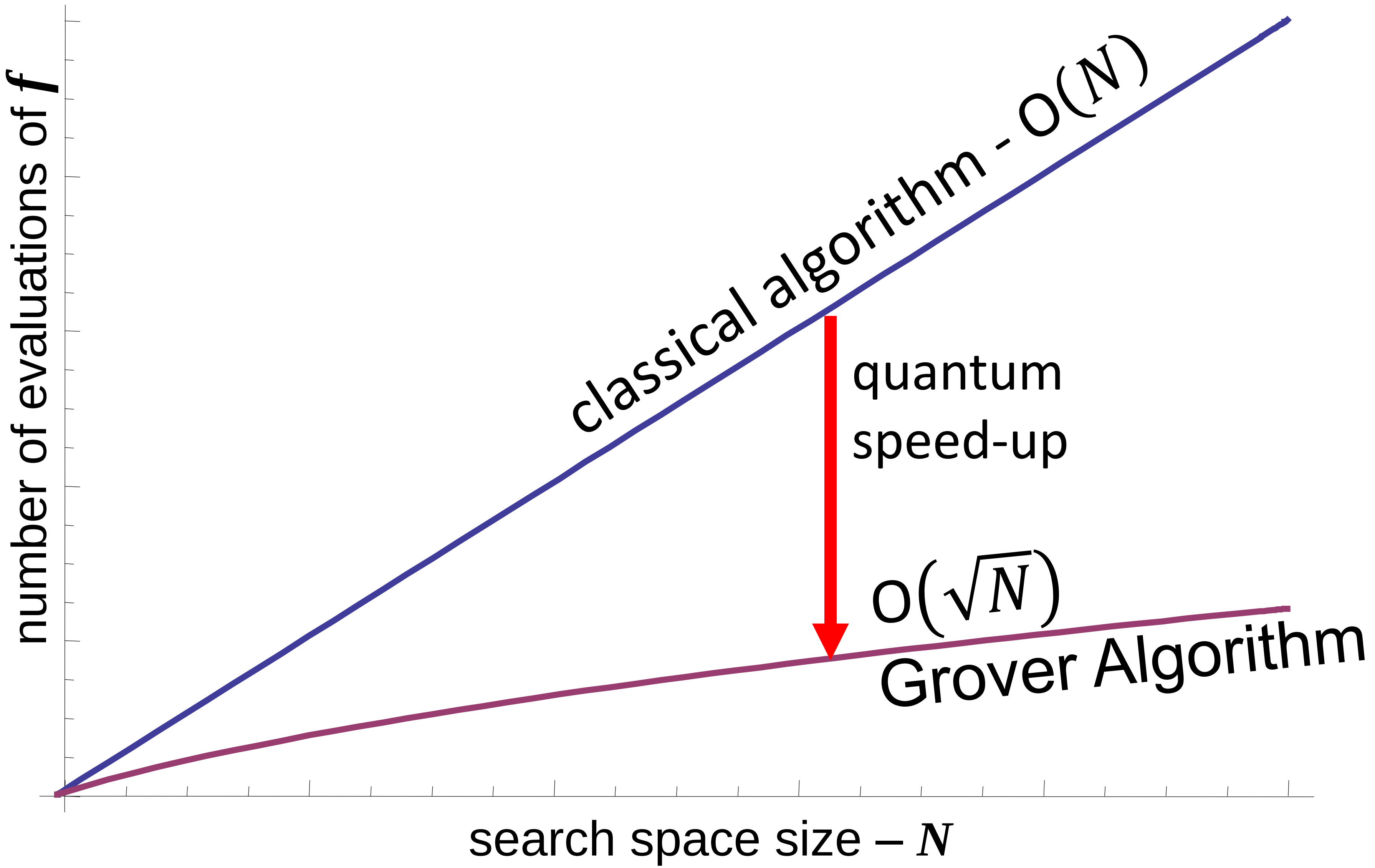
Grover L.K.: A fast quantum mechanical algorithm for database search, Proceedings, 28th Annual ACM Symposium on the Theory of Computing, 1996

Efficiency of Grover Search
(for 10 qubits)

≈ **25** iterations required

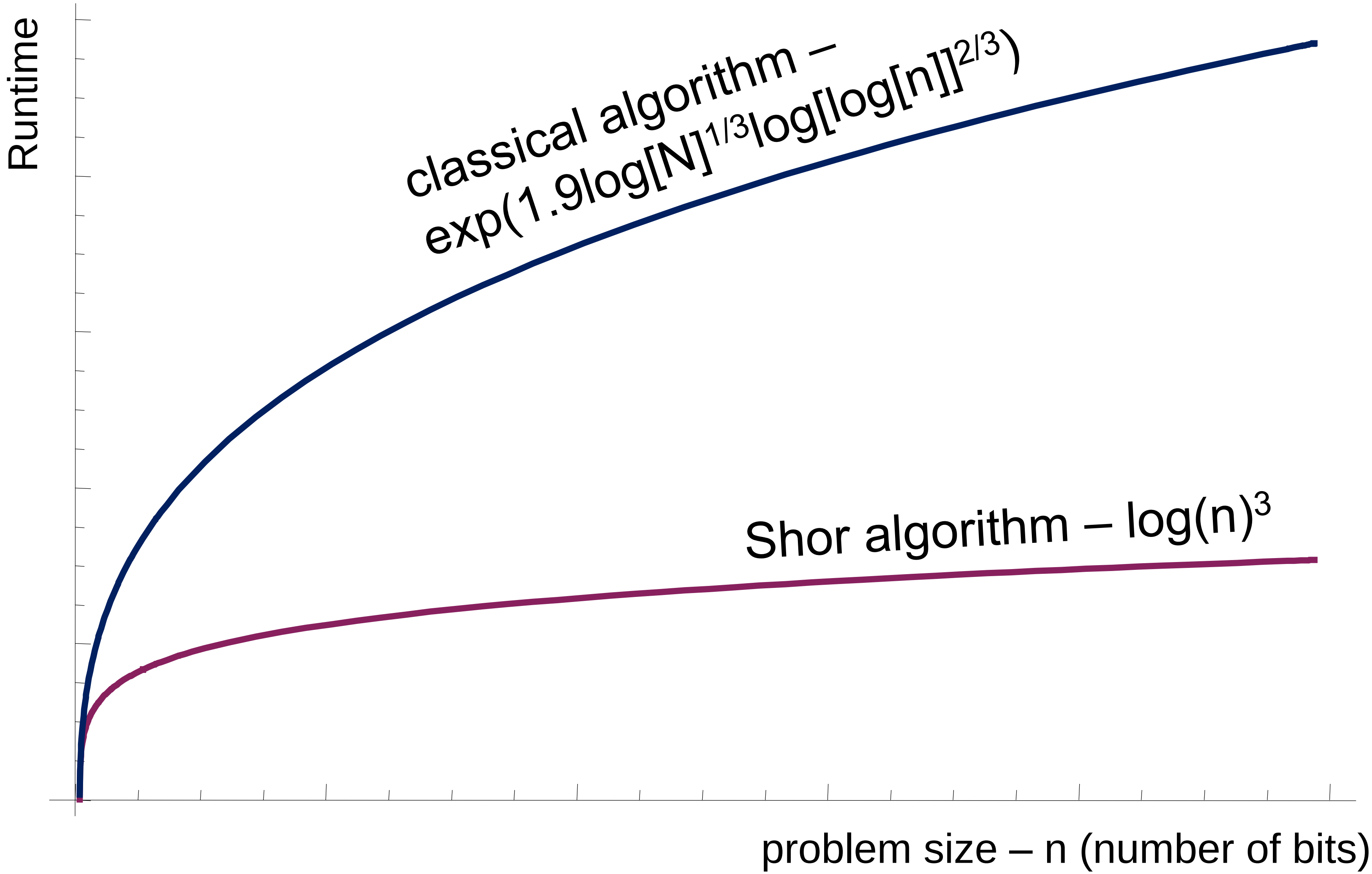


Time Complexity Revisited



Number Factorization: Shor Alg.

$r = q \cdot s$; q,s prime numbers



How to Build a Quantum Processor?

University of Innsbruck (http://www.quantumoptics.at/)

photo not CC-licensed

Ion Trap Quantum Processors

University of Santa Barbara (http://web.physics.ucsb.edu/~martinisgroup/)

photo not CC-licensed

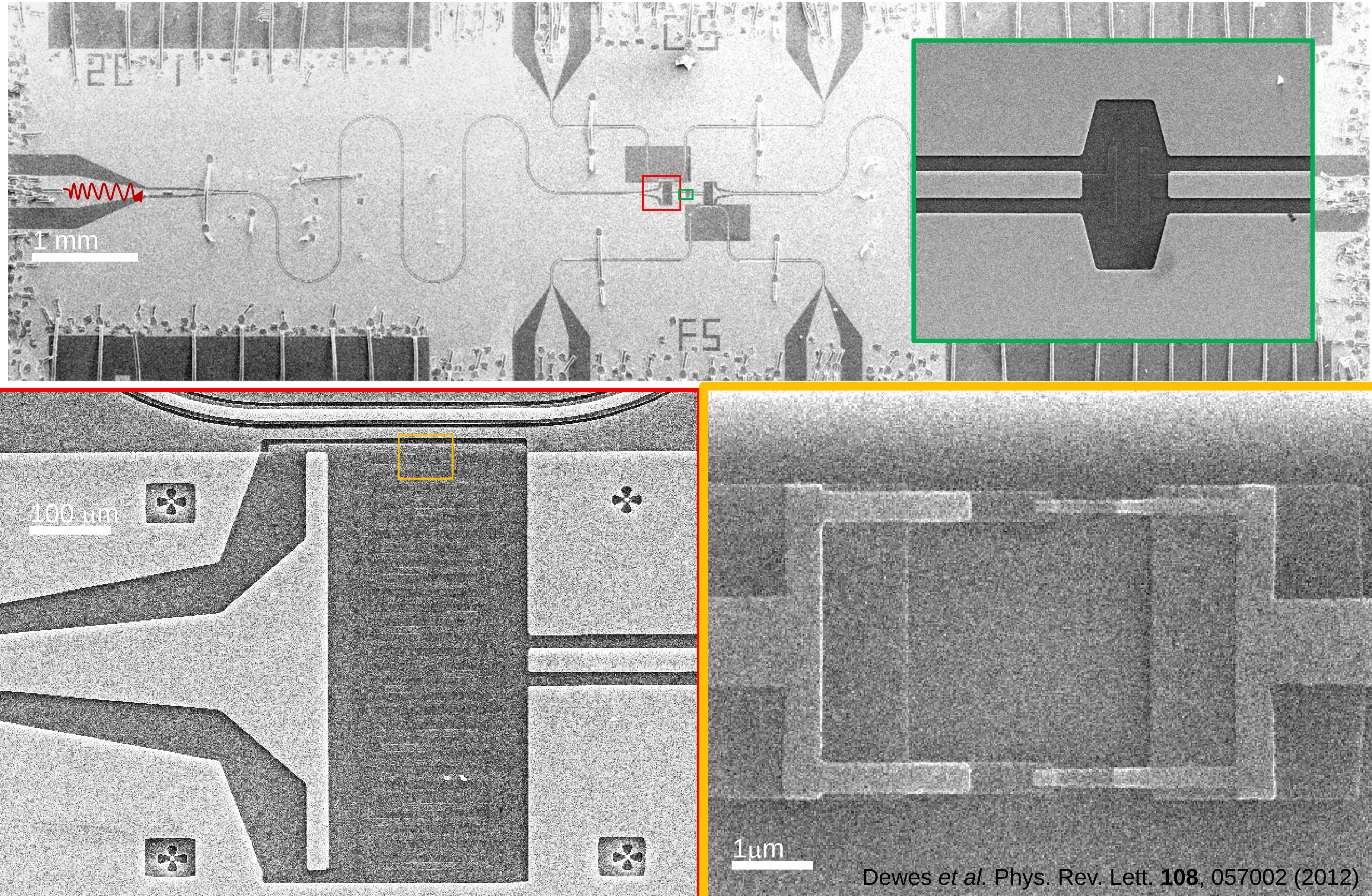
Superconducting Quantum Processors

...and many more technologies:

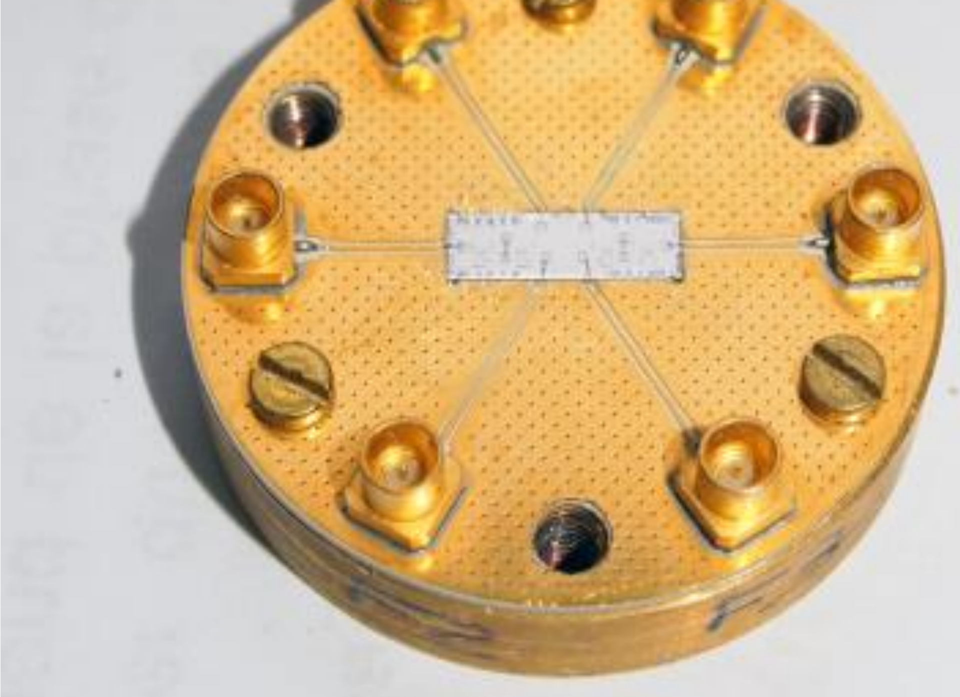
Nuclear magnetic resonance,
photonic qubits, quantum dots,
electrons on superfluid helium,
Bose-Einstein condensates...

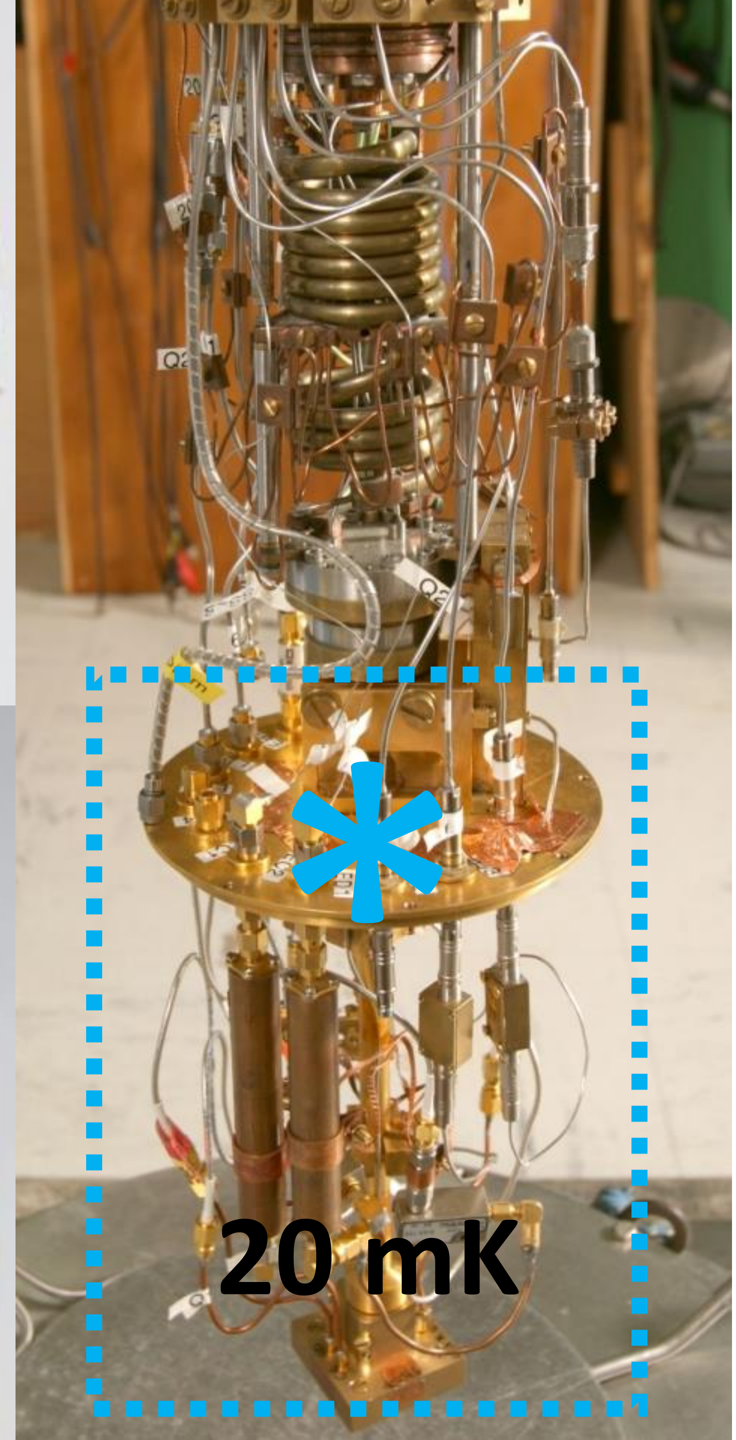
A Simple Two-Qubit Processor

Using superconducting qubits (Transmons - Wallraff *et al.*, Nature **431** (2004))



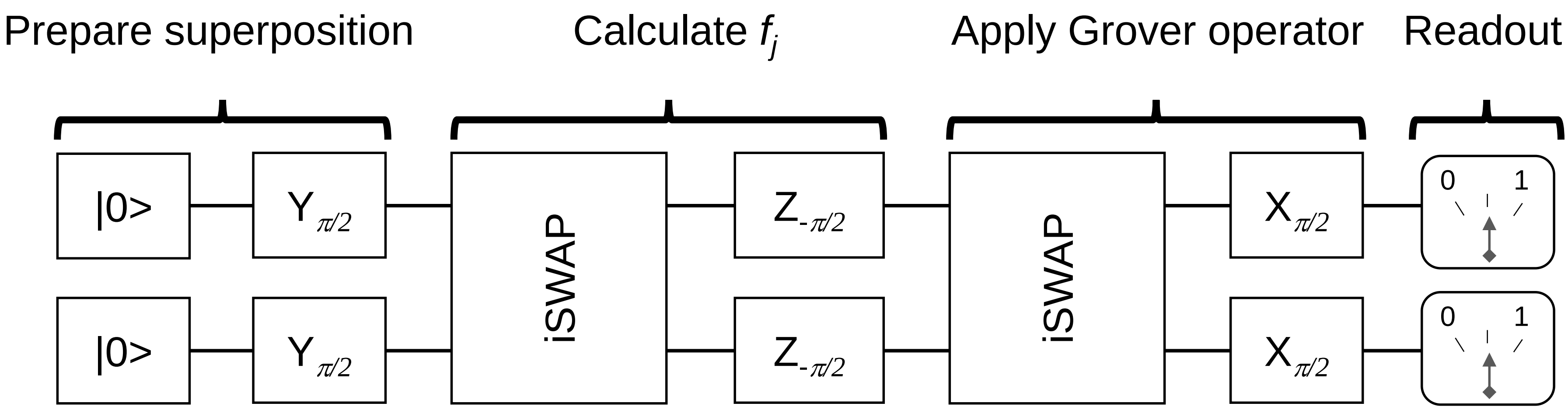
Dewes *et al.* Phys. Rev. Lett. **108**, 057002 (2012)

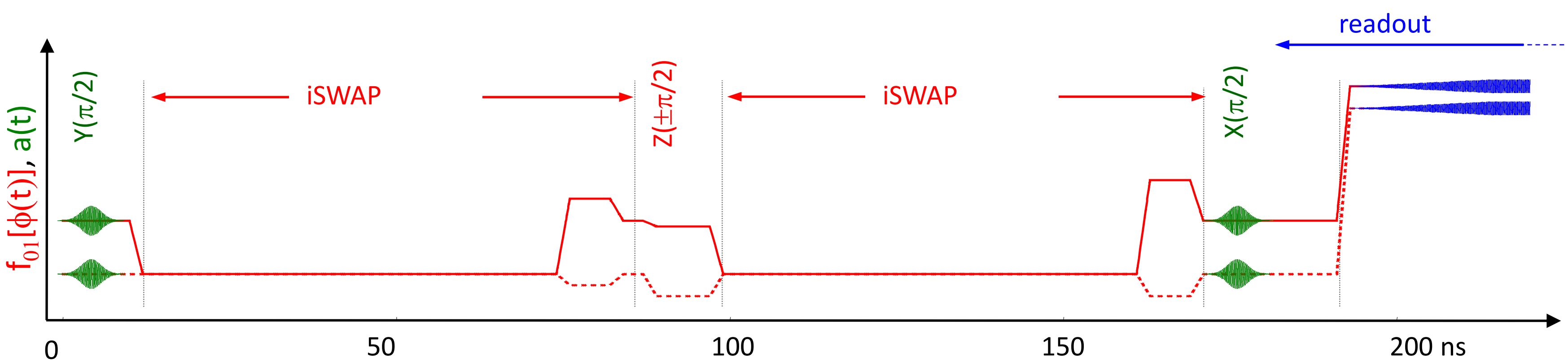




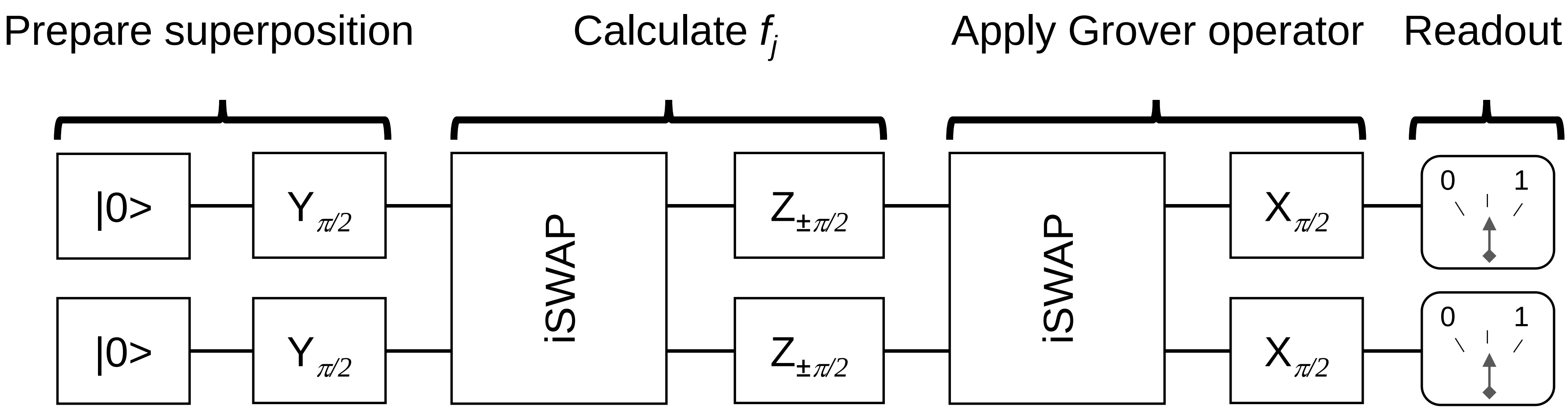
put in dilution cryostat

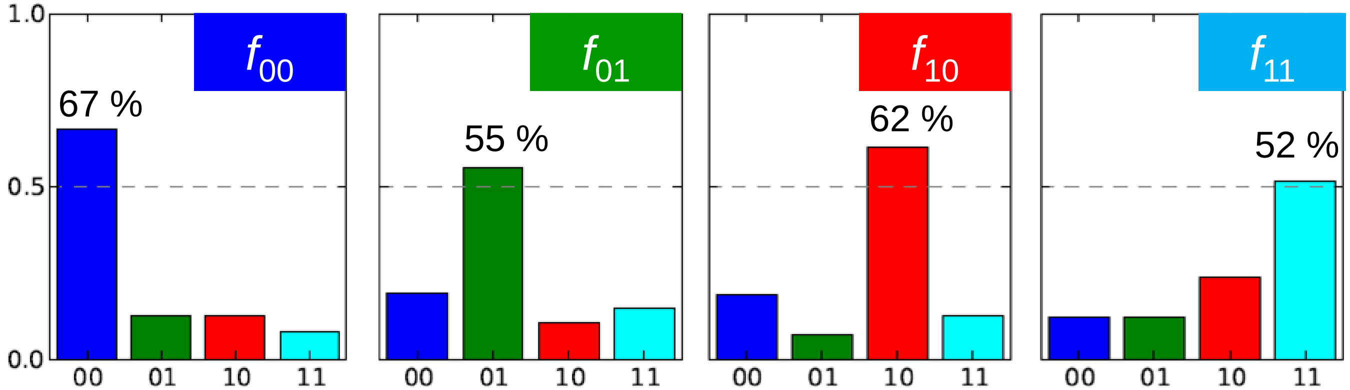
Running Grover-Search for 2 Qubits





Single-Run Success Probability





classical benchmark
(with "I'm feeling lucky" bonus)

Dewes et. al., PRB Rapid Comm **85** (2012)

Challenges

Decoherence

Environment measures and manipulates the qubit and destroys its quantum state.

Gate Fidelity & Qubit-Qubit Coupling

Difficult to reliably switch on & off qubit-qubit coupling with high precision for many qubits

And some more:

High-Fidelity state measurement, qubit reset, ...

Recent Trends in Superconducting Quantum Computing

Better Qubit Architectures

Better Qubits and Resonators

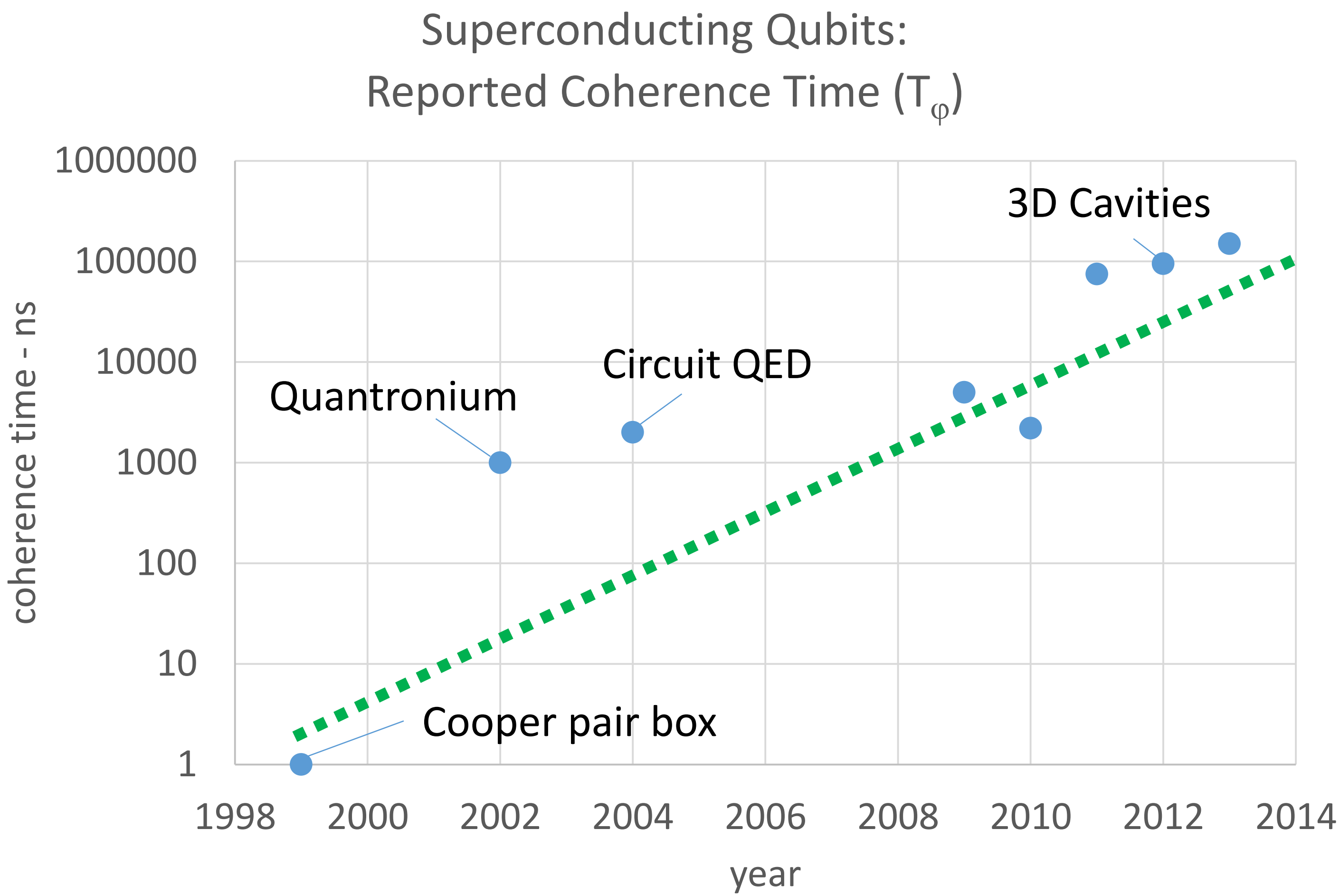
Quantum Error Correction

Hybrid Quantum Systems

(photos not included since not CC-BY licensed)

Moore's Law: Quantum Edition

(for superconducting qubits)



Summary

Quantum computers are coming!

...but still there are many engineering challenges to overcome...

Bad News

Likely that governments and big corporations will be in control of QC in the short term.

Thanks!

More "quantum information":

Diamonds are a quantum computer’s best friend –
Tomorrow, 30.12 at 12:45h in Hall 6 by Nicolas Wöhrl

Get in touch with me:
ich@andreas-dewes.de // @japh44