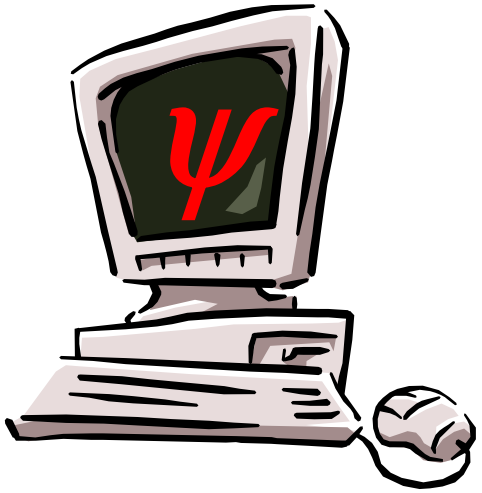


Scientific and technological challenges for the quantum computer

Zeno TOFFANO

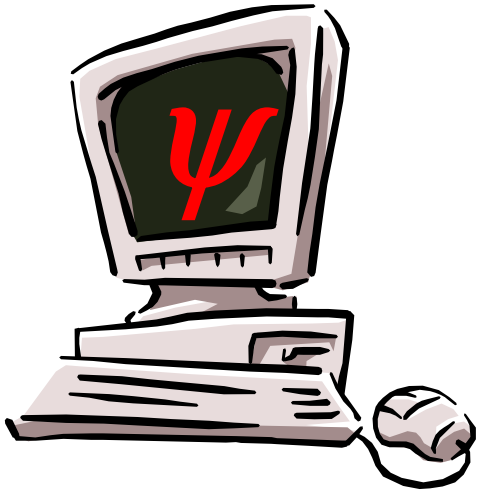
CentraleSupélec, Laboratoire des Signaux et Systèmes - CNRS (UMR8506),
Université ParisSaclay, Gif-sur-Yvette 91190, France

zeno.toffano@centralesupelec.fr

université PARIS-SACLAY

CentraleSupélec

cnrs



Défis scientifiques et technologiques pour l'ordinateur quantique

Zeno TOFFANO

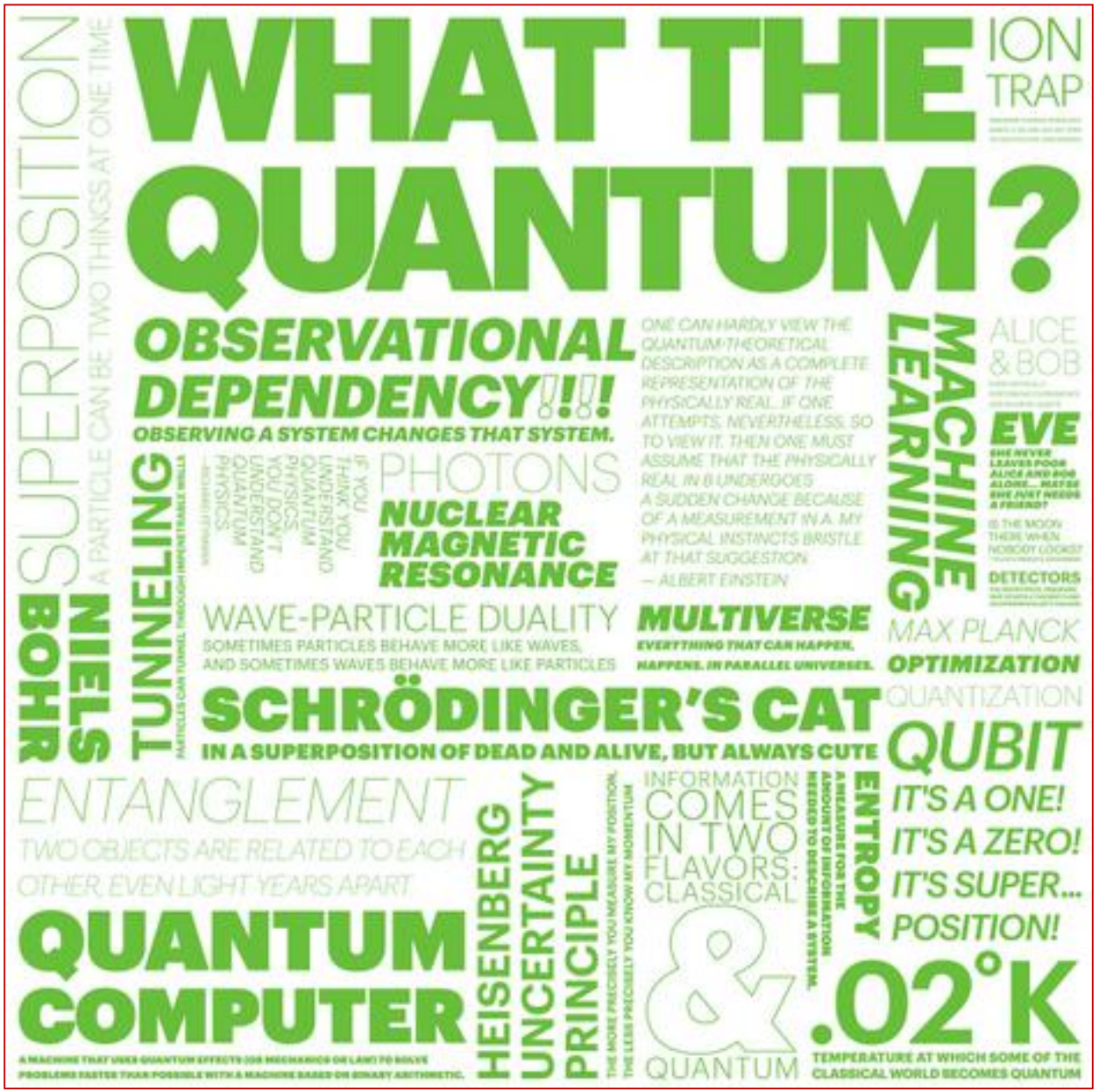
CentraleSupélec, Laboratoire des Signaux et Systèmes - CNRS (UMR8506),
Université ParisSaclay, Gif-sur-Yvette 91190, France

zeno.toffano@centralesupelec.fr

université PARIS-SACLAY

CentraleSupélec

cnrs


WHAT THE QUANTUM?
ION TRAP
SUPERPOSITION
A PARTICLE CAN BE TWO THINGS AT ONE TIME
OBSERVATIONAL DEPENDENCY!!!
OBSERVING A SYSTEM CHANGES THAT SYSTEM.
ONE CAN HARDLY VIEW THE QUANTUM-THEORETICAL DESCRIPTION AS A COMPLETE REPRESENTATION OF THE PHYSICALLY REAL. IF ONE ATTEMPTS, NEVERTHELESS, SO TO VIEW IT, THEN ONE MUST ASSUME THAT THE PHYSICALLY REAL IN B UNDERGOES A SUDDEN CHANGE BECAUSE OF A MEASUREMENT IN A. MY PHYSICAL INSTINCTS BRISTLE AT THAT SUGGESTION.
— ALBERT EINSTEIN
MACHINE LEARNING
ALICE & BOB
EVE
SHE NEVER LEAVES POOR ALICE AND BOB ALONE... MAYBE SHE JUST NEEDS A FRIEND!
IS THE MOON THERE WHEN NOBODY LOOKS?
DETECTORS
TUNNELING
PARTICLES CAN TUNNEL THROUGH IMPENETRABLE WALLS
IF YOU THINK YOU UNDERSTAND QUANTUM PHYSICS, YOU DON'T UNDERSTAND QUANTUM PHYSICS.
PHOTONS
NUCLEAR MAGNETIC RESONANCE
BOHR
NIELS
WAVE-PARTICLE DUALITY
SOMETIMES PARTICLES BEHAVE MORE LIKE WAVES, AND SOMETIMES WAVES BEHAVE MORE LIKE PARTICLES
MULTIVERSE
EVERYTHING THAT CAN HAPPEN, HAPPENS. IN PARALLEL UNIVERSES.
MAX PLANCK
OPTIMIZATION
QUANTIZATION
SCHRÖDINGER'S CAT
IN A SUPERPOSITION OF DEAD AND ALIVE, BUT ALWAYS CUTE
QUBIT
IT'S A ONE!
IT'S A ZERO!
IT'S SUPER...
POSITION!
ENTANGLEMENT
TWO OBJECTS ARE RELATED TO EACH OTHER EVEN LIGHT YEARS APART
HEISENBERG UNCERTAINTY PRINCIPLE
THE MORE PRECISELY YOU MEASURE MY POSITION, THE LESS PRECISELY YOU KNOW MY MOMENTUM
INFORMATION COMES IN TWO FLAVORS: CLASSICAL & QUANTUM
ENTROPY
A MEASURE FOR THE AMOUNT OF INFORMATION NEEDED TO DESCRIBE A SYSTEM.
QUANTUM COMPUTER
A MACHINE THAT USES QUANTUM EFFECTS (OR MECHANICS OR LAW) TO SOLVE PROBLEMS FASTER THAN POSSIBLE WITH A MACHINE BASED ON BINARY ARITHMETIC.
.02°K
TEMPERATURE AT WHICH SOME OF THE CLASSICAL WORLD BECOMES QUANTUM

quantum information

quantum circuits

entanglement

quantum computation

physical implementations

quantum algorithms

decoherence

quantum error correction

quantum communication

quantum measurements

quantum control

quantum simulation

quantum games

quantum cryptography QKD

quantum mechanics is based on axioms

- The **quantum state**, also named wave function or Ket $|\psi\rangle$ is a normalised vector in Hilbert space where the scalar product is defined

- A **measurement** made on a quantum system leads by an irreversible wavefunction collapse to a new quantum state. This process is described by a probability rule : the Born rule.

- A quantum state can be characterised by its **time evolution** described by a unitary operator in time t : $\boldsymbol{U}(t) = e^{-i\frac{\boldsymbol{H}t}{\hbar}}$

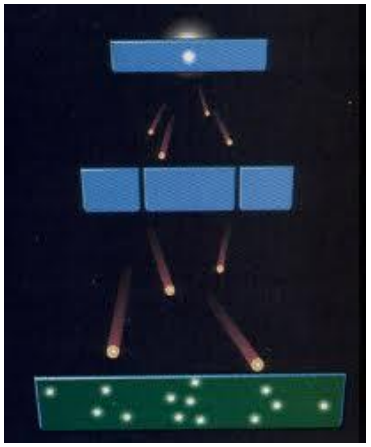
  $\boldsymbol{H}$ is the Hamiltonian operator and $\hbar$ the Planck's constant

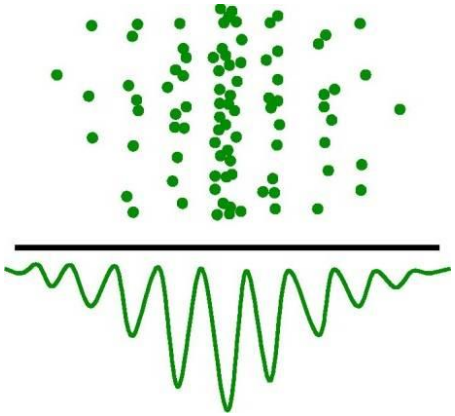
- **Composition**: a composite quantum system (multi-qubit) is the tensor product of the individual n states:

$$|\Psi\rangle = |\psi_1\psi_2 \dots \psi_n\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \dots \otimes |\psi_n\rangle$$

quantum state: particle or wave ?

Particle interference experiments: Young's slits





So everything is both particle and wave. **troubling !?**

Bohr's **Complementarity principle**:

It is not possible to describe physical "observable" simultaneously both in terms of particles and in terms of waves.

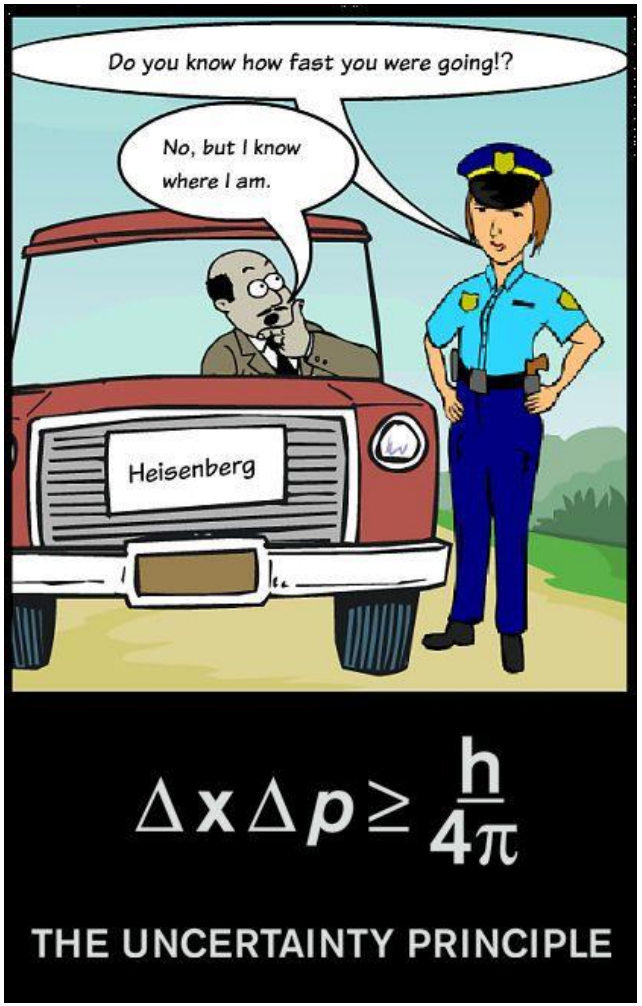
Heisenberg's uncertainty principle

The position ***x*** and momentum ***p*** (speed) of a particle that you measure will depend on the sequence in which you measure them.

This is the reason why you cannot measure *both* position and momentum of a quantum particle with absolute accuracy: uncertainty Δx and Δp.

This says that the observables ***X*** and ***P*** are incompatible and complemantary

The mathematical property is the **non-commutativity** of the observables



quantum computing

Classical Input

$|\psi_{\text{in}}\rangle$

QUANTUM WORLD

$|\psi_{\text{out}}\rangle$

Classical Output

historical milestones

- 1980 – **Paul Benioff** proposes the therethical concept of Hamiltonians as Turing Machines
- 1982 – **Richard Feynman** proposed the idea of creating machines based on the laws of quantum mechanics instead of the laws of classical physics.
- 1985 – **David Deutsch** developed the quantum turing machine, showing that quantum circuits are universal.
- 1994 – **Peter Shor** came up with a quantum algorithm to factor very large numbers in polynomial time.
- 1997 – **Lov Grover** develops a quantum search algorithm with $O(\sqrt{N})$ complexity
- 1998 – **First 2 qubit quantum computing system** developed, was only able to do some simple calculations by using the principle of nuclear magnetic resonance NMR.

Paul A. Benioff was honored for his pioneering work that **first proved** that quantum computing was a theoretical possibility.

Journal of Statistical Physics, Vol. 22, No. 5, 1980

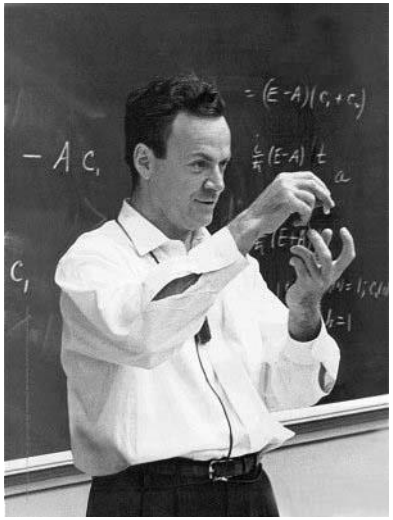
The Computer as a Physical System: A Microscopic Quantum Mechanical Hamiltonian Model of Computers as Represented by Turing Machines

Paul Benioff[1,2]

Received June 11, 1979; revised August 9, 1979

KEY WORDS: Computer as a physical system; microscopic Hamiltonian models of computers; Schrödinger equation description of Turing machines; Coleman model approximation; closed conservative system; quantum spin lattices.

In this paper a microscopic quantum mechanical model of computers as represented by Turing machines is constructed. It is shown that for each



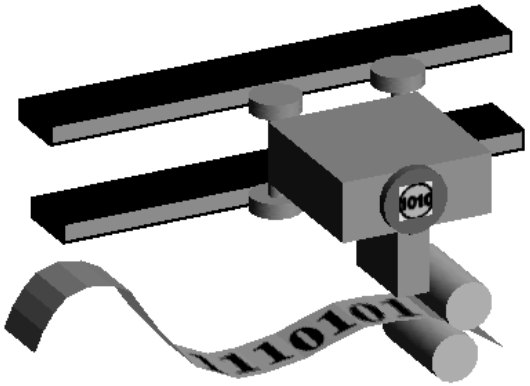
Richard Feynman (1982) :

“...trying to find a computer simulation of physics, seems to me to be an excellent program to follow out...and I'm not happy with all the analyses that go with just the classical theory, because *nature isn’t classical*, dammit, and if you want to make a simulation of nature, you'd better *make it quantum mechanical*, and by golly it's a wonderful problem because it doesn't look so easy.”

Simulating physics with computers,
Int. J. Theor. Phys. **21**, 467 (1982).

universal computation

Turing machines.



Church-Turing thesis:

A computable function is one that is computable by a universal Turing machine.

David Deutsch (1985) :

"Computing machines resembling the universal quantum computer could, in principle, be built and would have many remarkable properties not reproducible by any Turing machine … Complexity theory for [such machines] deserves further investigation."

Quantum theory, the Church-Turing principle and the universal quantum computer.
Proc. R. Soc. A 1985, 400, 97–117.

the power of quantum computation

- In quantum systems possibilities count, even if they never happen!

- Each of exponentially many possibilities can be used to perform a part of a computation at the same time.

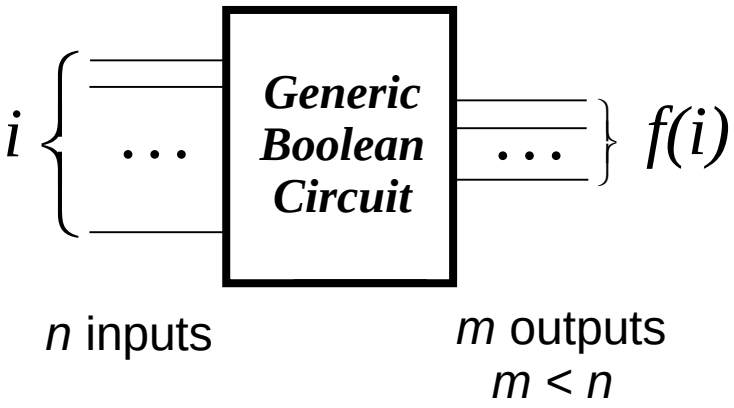
reversible logical circuits

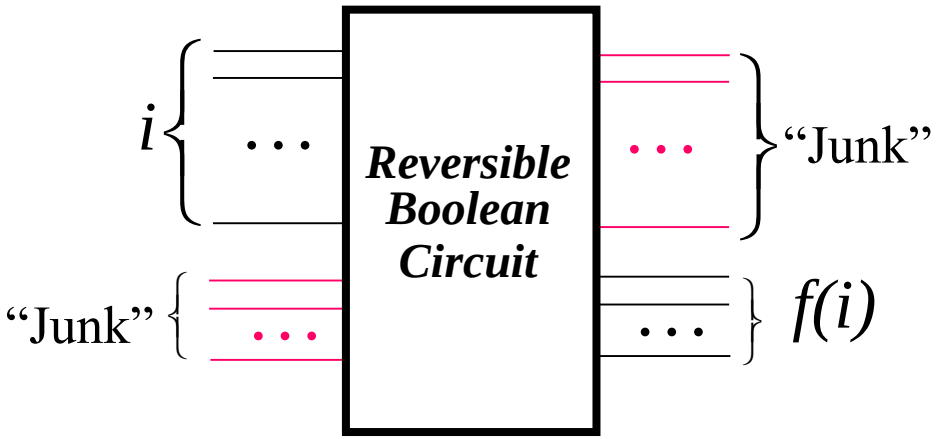
- Reversibility was studied around 1980 motivated by power minimization considerations.
  - **Landauer**'s principle: each "wire' suppression in a circuit dissipates an energy amount of $kT\ \mathrm{Ln}2$

    very small energy ε : at ambient temperature $T = 300k$

    $\varepsilon \approx 3\ 10^{-21}$ joule / 0.02 eV

- **Bennett**, **Toffoli** *et al.* showed that any classical logic circuit can be made reversible with modest overhead.





the qubit

A **qubit** (quantum bit) can be put into a superposition of two defined states $|0\rangle$ and $|1\rangle$ (classical bits)

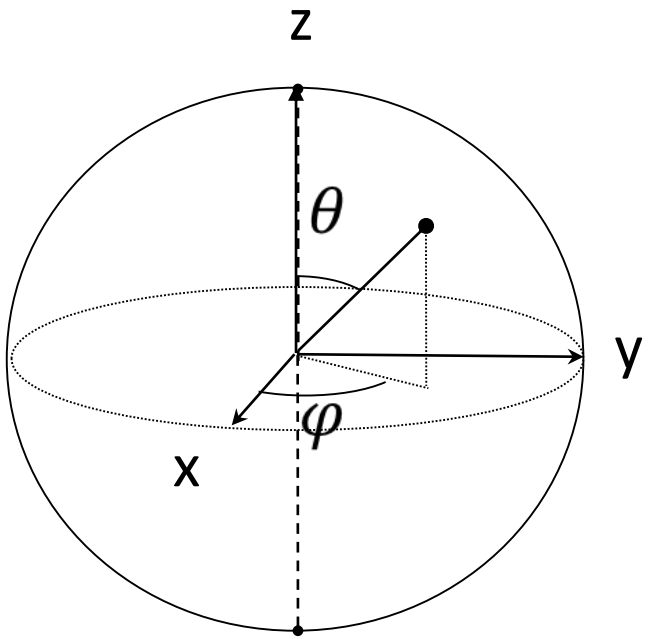
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

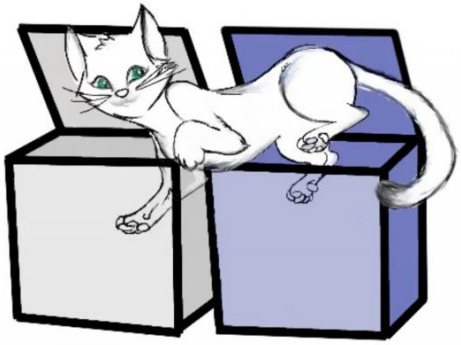
not only two possible bit states but an infinity.

α and β are two complex numbers giving the probabilities $|\alpha|^2 + |\beta|^2 = 1$.

The qubit "lives" on a unit sphere (**Bloch sphere**) with

$$\alpha = \cos\frac{\theta}{2} \quad \text{and} \quad \beta = e^{+i\varphi}\sin\frac{\theta}{2}$$





quantum superposition

Schrödinger's cat

BOTH DEAD AND ALIVE

"en même temps"

+ and − for quantum computing

The important **quantum resources** that come into play in the building of a quantum computer are principally:

\+ Superposition

\+ Entanglement

On the other side a drawback necessitating error correction is:

\- Decoherence

quantum entanglement: no cloning, no deletion

If you do not know the state of a quantum system then you cannot make an exact copy of it :

no-cloning theorem

Unless a quantum system collapses, you cannot delete information in a quantum system:

no-deletion theorem

These results are connected with the quantum phenomenon of **entanglement**.

Quantum algorithms make very clever use of quantum superposition and quantum entanglement.

quantum circuit

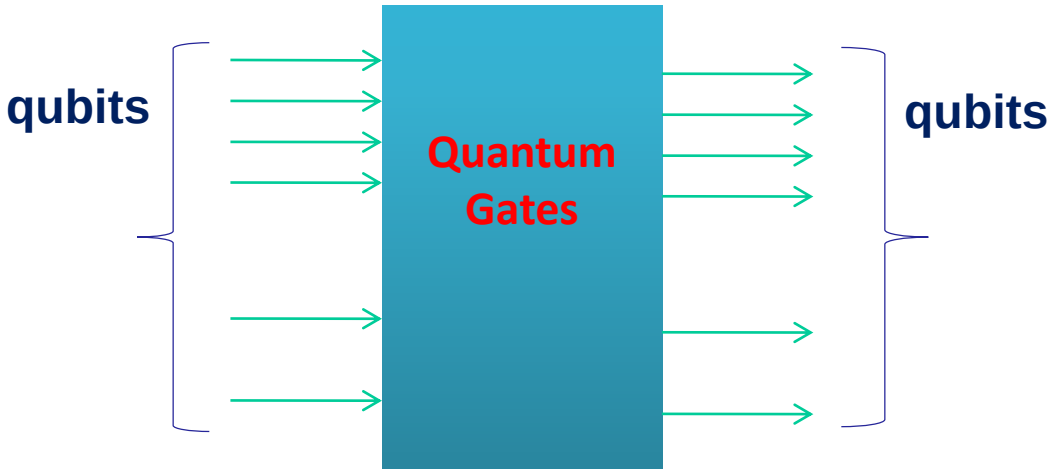
- Unitary Operations

- Reversible gates and circuits (information-lossless)
  - Number of output signal lines = Number of input lines
  - The output vectors are a permutation of the input vectors

- Logic used in computation
  - **Classical logic** behavior: permutation matrices
  - **Non-classical logic** behavior: state sign (phase) and entanglement

Object: **qubit**

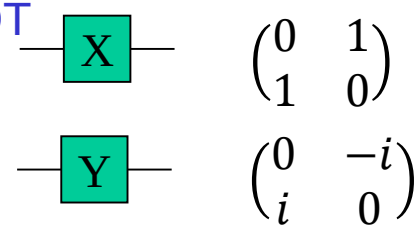
Operation: **quantum gate**



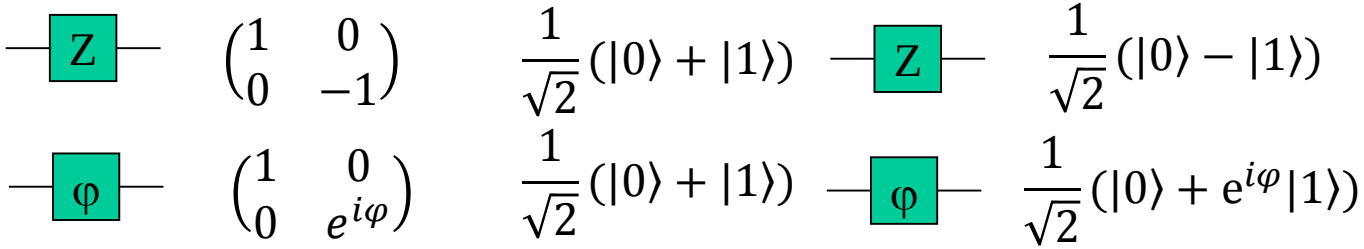
one-qubit operations

computational basis: $\{|0\rangle, |1\rangle\}$

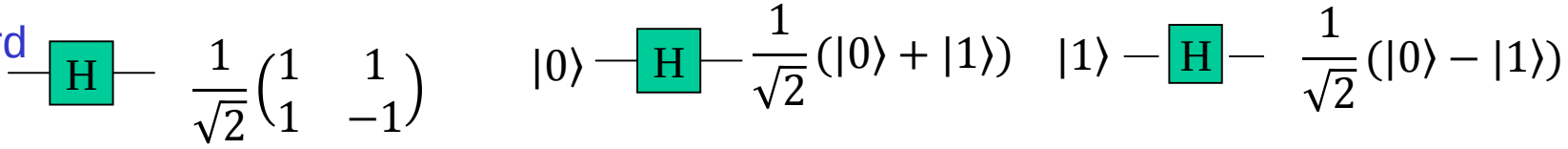
NOT



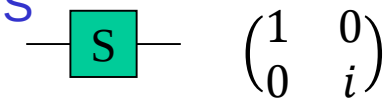
Phase



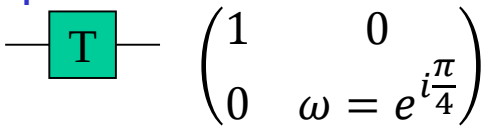
Hadamard



Clifford S



Non-Clifford T

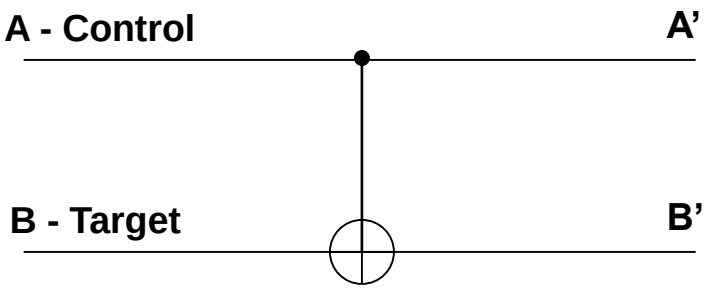


two-qubit operation : CNOT

A gate operating on two qubits is called **CNOT** (*Controlled-NOT).*

It has an entangling power meaning that it is a non-local quantum gate

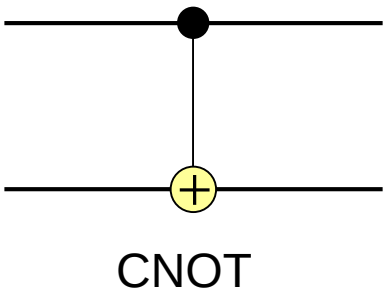
If the bit on the control line is 1, invert the bit on the target line.



Input		Output	
A	B	A'	B'
0	0	0	0
0	1	1	1
1	0	1	0
1	1	0	1

Note: The CNOT gate has a similar behavior to the logical XOR gate, (B'=B⊕A), with some extra information to make it reversible.

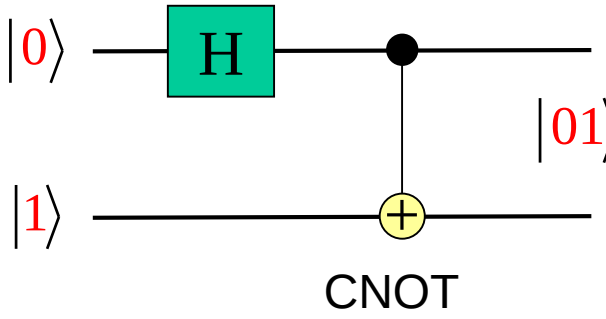
CNOT gate matrix



$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$|00\rangle \xrightarrow{CNOT} |00\rangle$$
$$|01\rangle \xrightarrow{CNOT} |01\rangle$$
$$|10\rangle \xrightarrow{CNOT} |11\rangle$$
$$|11\rangle \xrightarrow{CNOT} |10\rangle$$

How to generate an entangled state (Bell state)

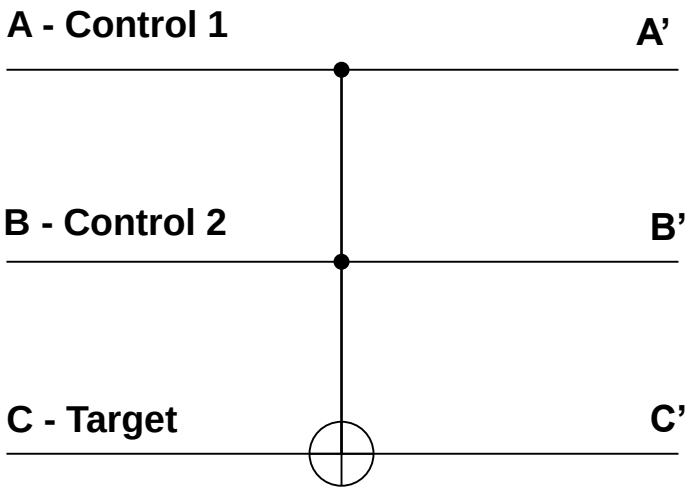


$$|01\rangle \xrightarrow{H_1} \frac{1}{\sqrt{2}}\left(|01\rangle + |11\rangle\right) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right) = \Psi^{(+)}$$

all in one: the Toffoli universal gate

The Toffoli (double-CNOT) gate is a **universal** reversible logic gate because it can be used as a NAND gate.

Universality in Logic: logical NAND generates all other arity-1 and arity-2 logical functions (NOT, AND, OR, NOR, XOR…)

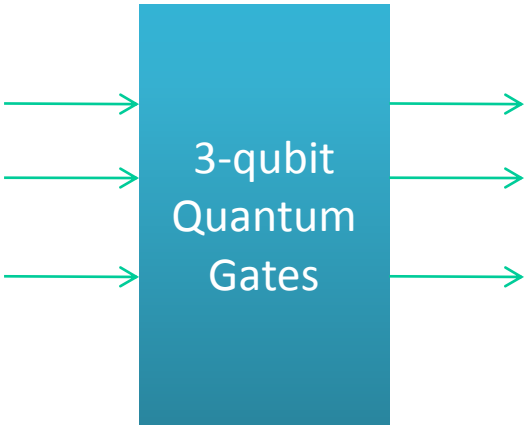


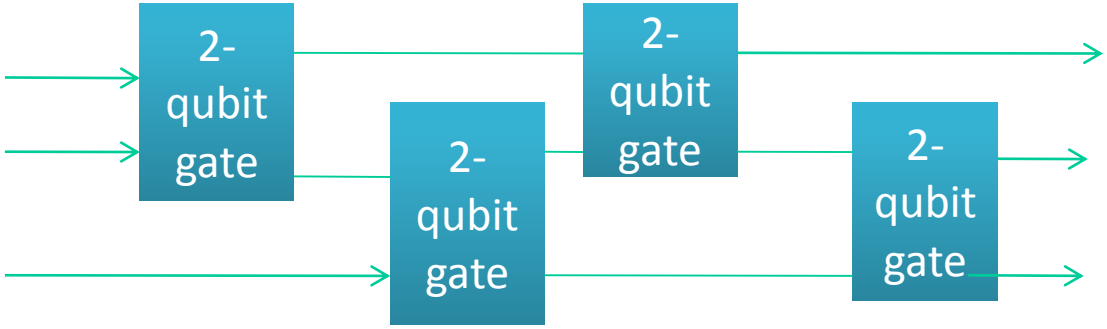
Input			Output		
A	B	C	A’	B’	C’
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Note: the target output is a result of a logical NAND gate of A and B when the target is C is at 1: $C' = C \oplus (A \wedge B)$

David DiVincenzo (1994):

An arbitrary N-qubit quantum gate can be expressed exactly as a sequence of products of some two-qubit gates.

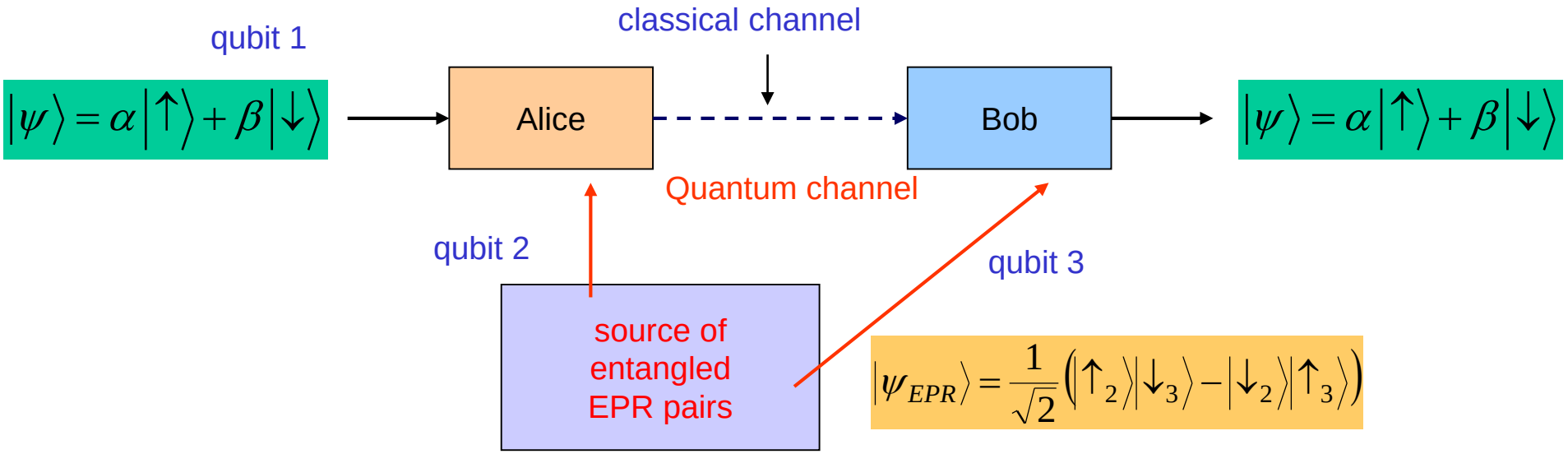




scenario for quantum teleportation

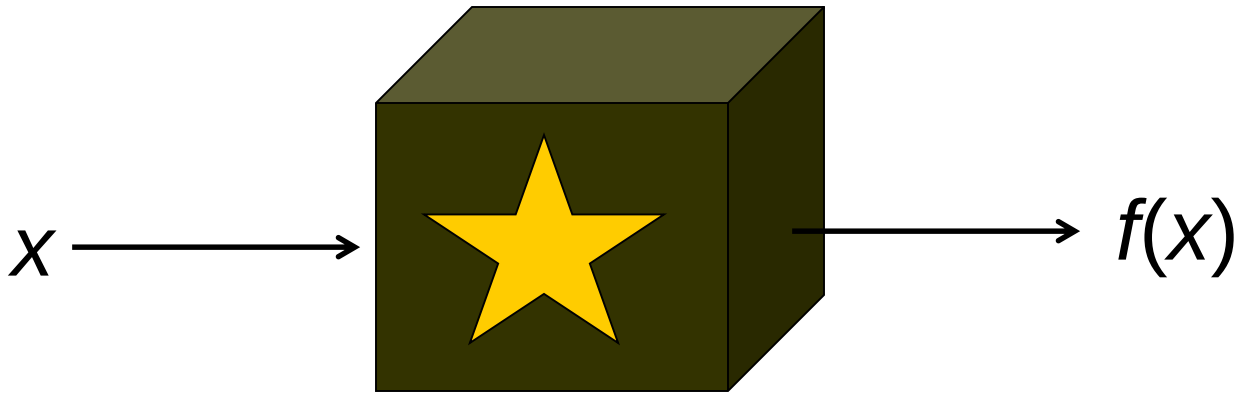
"Gentlemen beam me aboard"

Captain Kirk



Simon's Problem

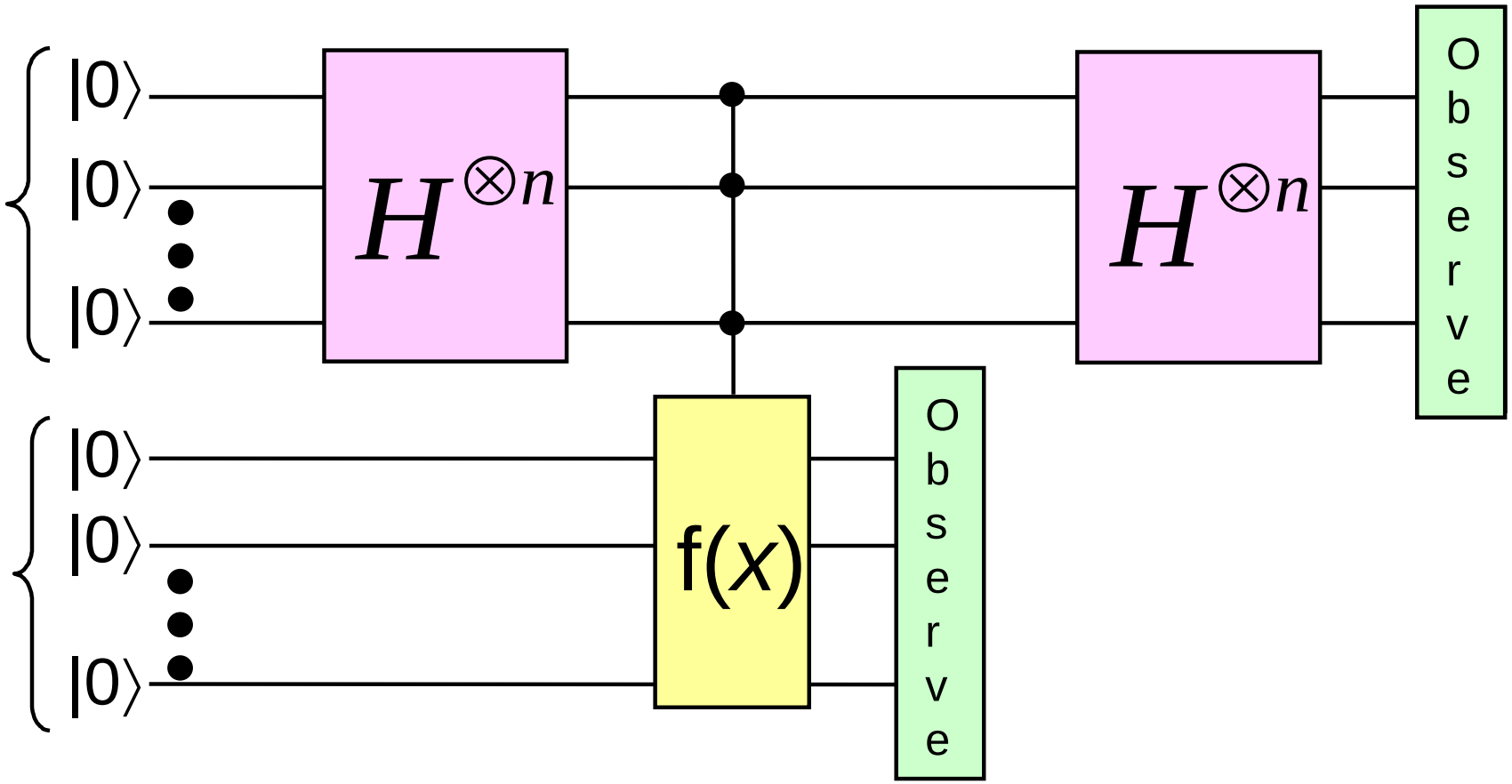
Given a **black box** (*oracle*)

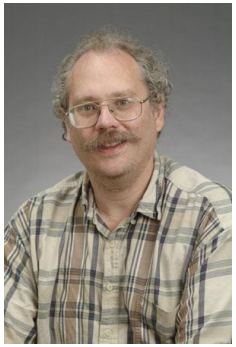


Promise: There exists a secret string s such that $f(x) = f(y) \Leftrightarrow y = x \oplus s$ for all x,y ($\oplus$: bitwise XOR)

Problem: Find s with as few queries as possible

Simon's problem: quantum circuit diagram





Shor's Algorithm

To Factor *N* on a quantum computer: select *x* coprime to *N.*
Use the quantum computer to find the period of

$$f(s) = x^s \bmod N$$

Use order of *x* to compute possible factors of *N*
using QFT (Quantum Fourier Transform).
Check if they work. If not rerun.

P. W. Shor. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", SIAM J. Computing 26, pp. 1484-1509, 1997.

188198812920607963838697239461650439807163563379417382700763356422988859715234665485319060606504743045317388011303396716199692321205734031879550656996221305168759307650257059

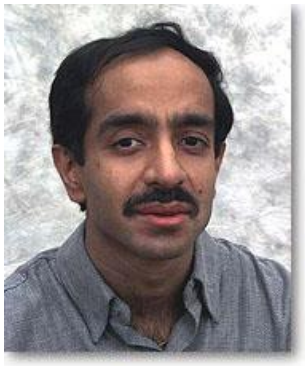
=

39807508642406493739712550055038649119906436234252670840638518957594638895726176858331747277214610743530253623071973048224632914695302097116459852171130520711256363590397527

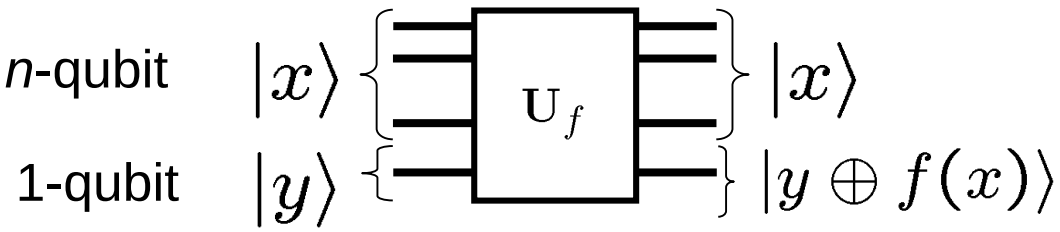
Best classical algorithm takes time $O(\exp(n^{1/3}))$

Shor's quantum algorithm takes time $O(n^3 \log n)$

Grover's Problem



Suppose we have a black box



with the property

$$f(x_0) = 1$$
$$\forall x \neq x_0, f(x) = 0$$

Problem: find x_0 with as few queries as possible.

Classical query: *O(N)* complexity
Quantum Grover query: *O(√N)* complexity

L. K. Grover. "A fast quantum mechanical algorithm for database search", Proceedings, 28th Annual ACM Symp. on the Theory of Computing, p. 212, 1996.

Di Vincenzo criteria for a quantum computer

These criteria represent the minimal behaviors needed to perform general-purpose quantum computing in the presence of likely architectural constraints.

Criteria 1. **Scalability**: a physical system that contains qubits must exist (Scalability implies capability to fabricate and layout as many register elements as needed for a specific computation)

Criteria 2. **Initialization**: capability to induce qubits to initialize with high fidelity (the starting quantum state of the computation must be well-known to ensure accurate results)

Criteria 3. **Read-out** of a register on a defined basis (the measurement samples the statistical distribution encoded by the quantum state)

Criteria 4. **Control** over a set of universal quantum gates (composing arbitrary gates from a finite, universal gate set)

Criteria 5. **Duration** of the gate sequence must be shorter than the characteristic decoherence time (fault-tolerant protocols using quantum error correction codes are designed to counter decoherence and other errors by redundantly encoding information)

requirements for a viable quantum computer

- realizing the algorithmic advantages of quantum computing requires hardware devices capable of encoding quantum information.
- For more than 35 years, there has been a broad array of experimental efforts to build quantum computing devices
- Multiple state-of-the-art engineering efforts have now fabricated functioning quantum processing units (QPUs) capable of carrying out small-scale demonstrations of quantum computing.

devices for quantum computing

There are many different possible technologies available for building quantum computers, and these are typically classified by how qubits of information are stored.

These technologies are based on different physical principles:

Superconductors

Ions in cavities

Lasers

Quantum dots

Photonics

NMR

Magnetic systems

Semiconductors

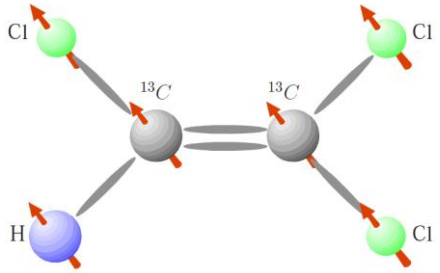
…

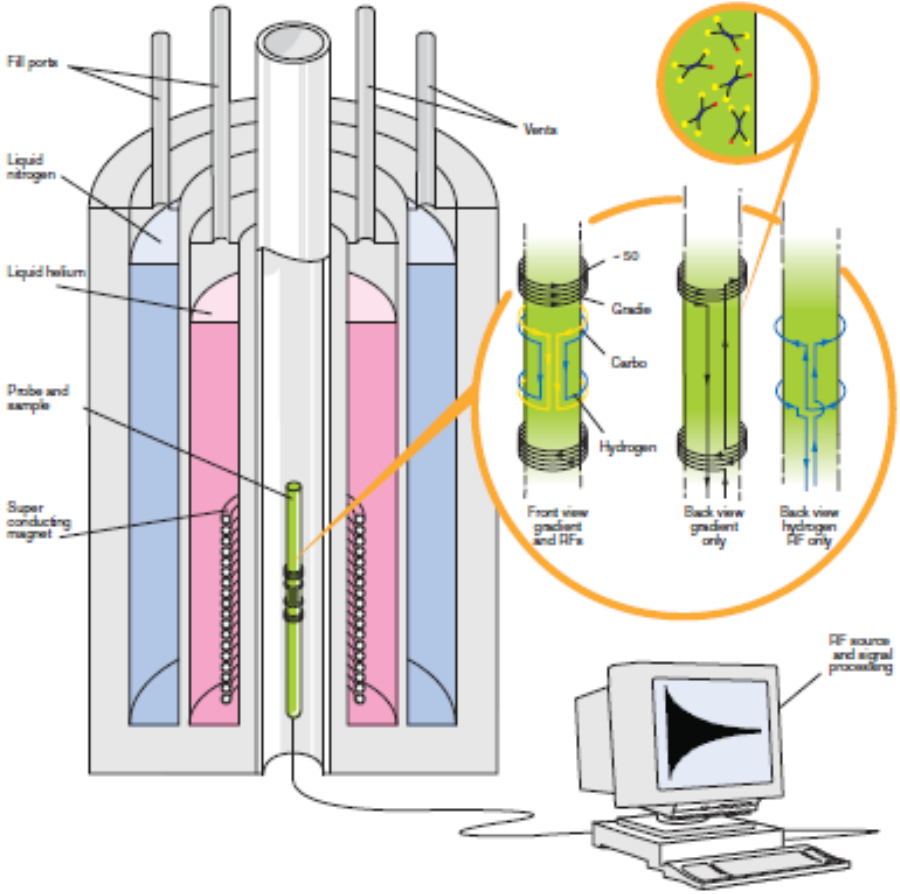
NMR (Nuclear Magnetic Resonance) qubits

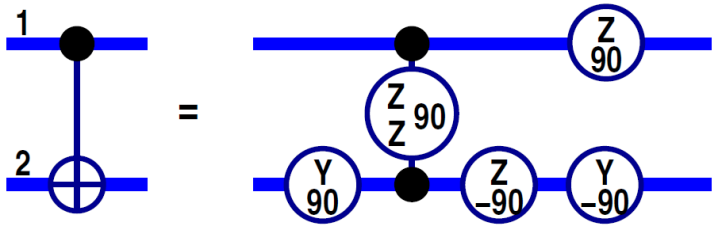
trichloroethylene

There are three useful nuclei for realizing qubits: the proton (H), and the two ^{13}C.

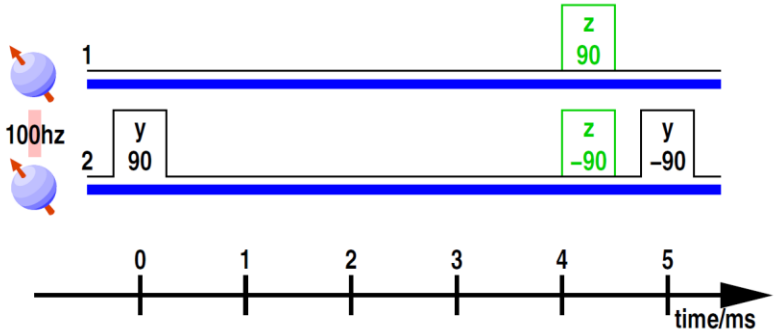
The normal isotope of carbon ^{12}C (spin-zero), is replaced by ^{13}C (spin ½).







Pulse sequence for realizing the CNOT

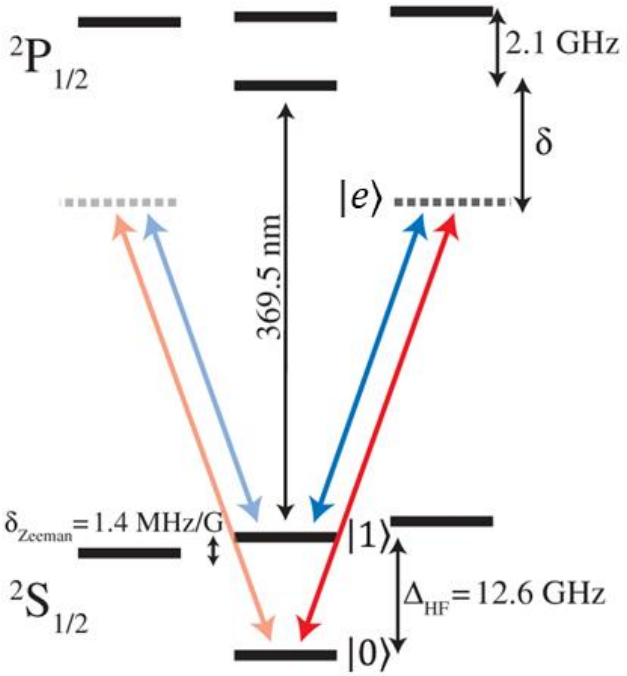


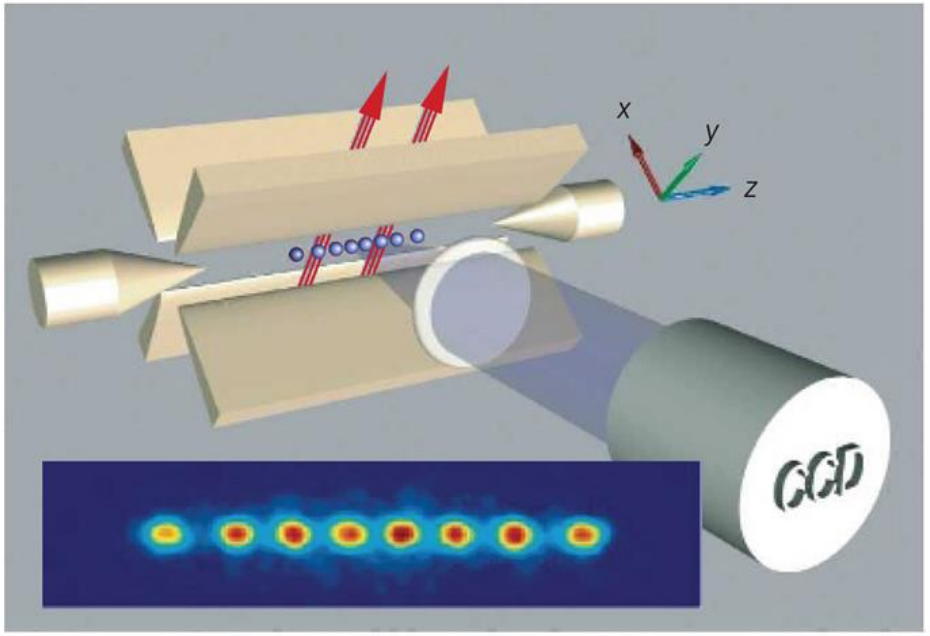
R. Laflamme, E. Knill & al , "Introduction to NMR Quantum Information Processing", arXiv:quant-ph/0207172

trapped ion qubits

Electronic energy levels of a $^{171}Yb^+$ ion illustrating qubit encoding ($|0\rangle$ and $|1\rangle$) with hyperfine energy levels.

Transition between qubit states is achieved by a Raman process via excitation to a virtual state $|e\rangle$.

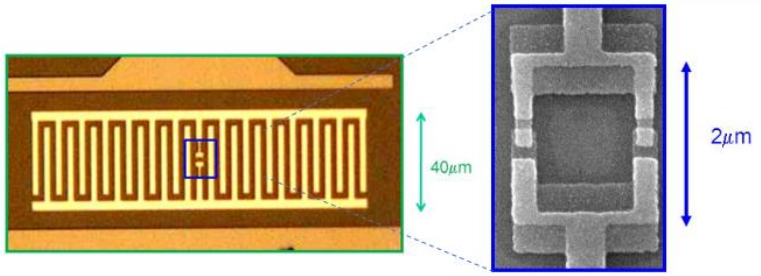




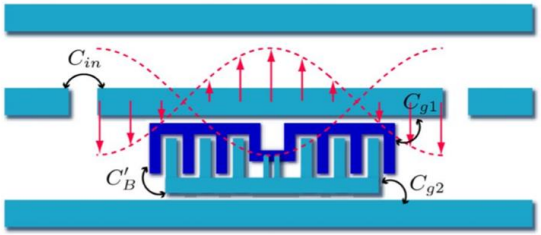
Schematic of a trap used to confine ions in vacuum. Inset : Visualization of ions in the trap with fluorescent techniques.

R. Blatt and D. Wineland, "Entangled states of trapped atomic ions," Nature, vol. 453, no. 7198, p. 1008, 2008.

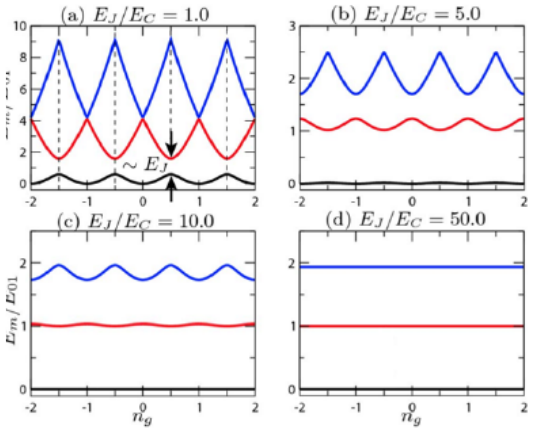
superconducting transmon qubits



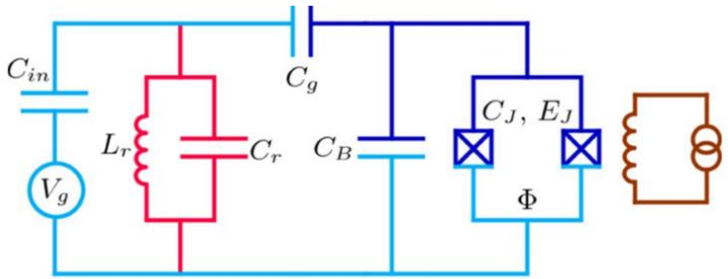
The transmon qubit consisting of two superconducting islands that are coupled through Josephson junctions and a large interdigitated capacitance.



Schematic of a transmon qubit capacitively coupled to a superconducting resonator for initialization, readout and control.



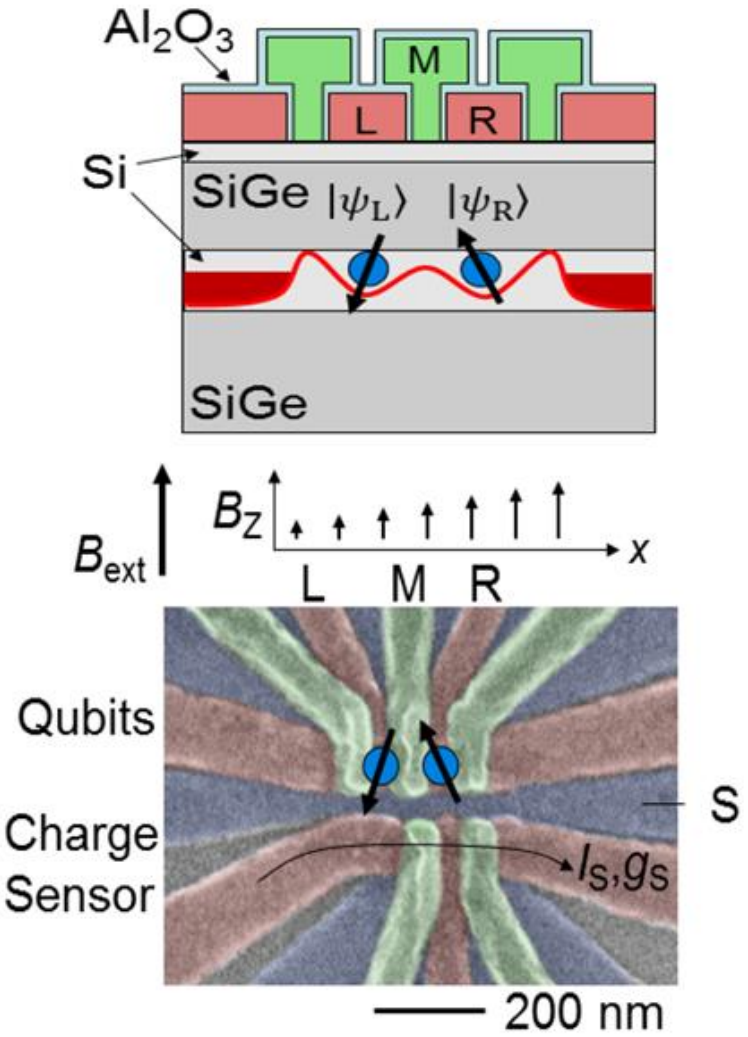
Eigenenergies (first three levels, m = 0,1,2) of the superconducting system function of the effective offset charge by nearby gate electrodes and environment. Energies are given in units of the transition energy.



Equivalent circuit of a transmon coupled to the resonator.

J. Koch, M. Y. Terri, J. Gambetta, A. A. Houck, D. Schuster, J. Majer, A. Blais, M. H. Devoret, S. M. Girvin, and R. J. Schoelkopf, "Charge insensitive qubit design derived from the cooper pair box," Physical Review A, vol. 76, no. 4, p. 042319, 2007.

Silicon spin qubits



Device schematic highlighting the position of the quantum dots.

Variation of the static magnetic field along a slice of the device.

SEM image of a Si/SiGe double quantum dot device, where two-qubit operations were implemented.

D. M. Zajac, A. J. Sigillito, M. Russ, F. Borjans, J. M. Taylor, G. Burkard, and J. R. Petta, "Resonantly driven cnot gate for electron spins," Science, vol. 359, no. 6374, pp. 439–442, 2018

photonic technologies

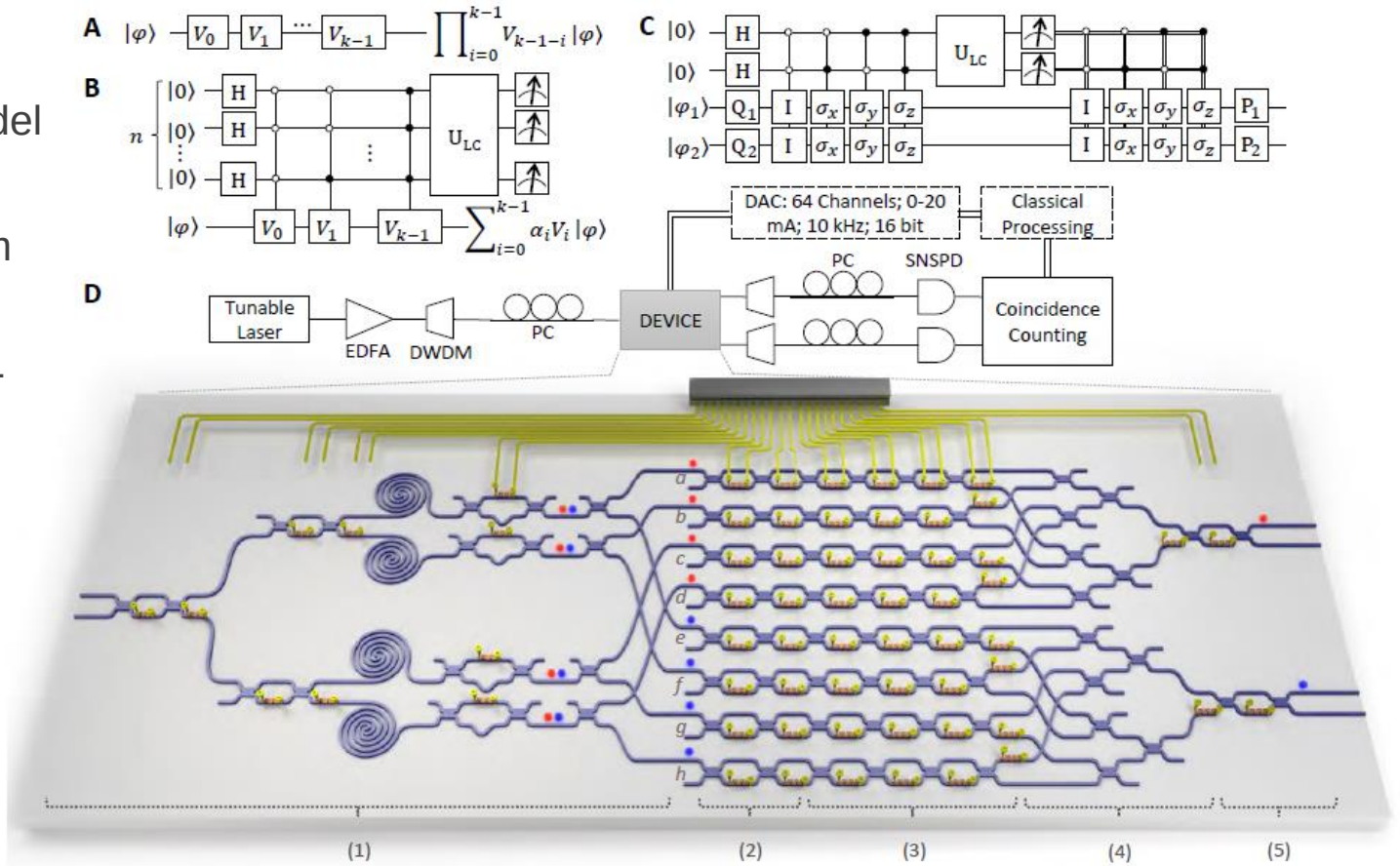
Quantum information processing circuits

(A) quantum circuit model

(B) Probabilistic linear-combination of quantum gates.

(C) Deterministic linear-combination circuit for universal two-qubit unitary operation.

(D) Schematic and external setup.

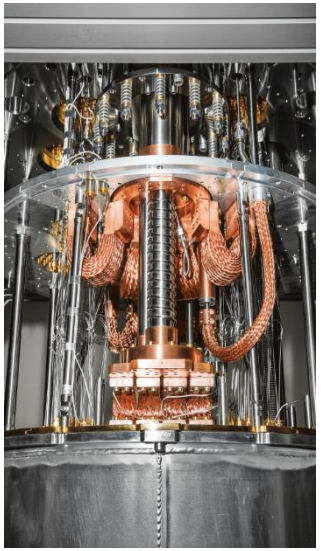


A tunable continuous wave laser is amplified with an optical fibre amplifier (EDFA), spectrally filtered by a dense wavelength division multiplexing (DWDM) module and launched into the device through a V-groove fibre array

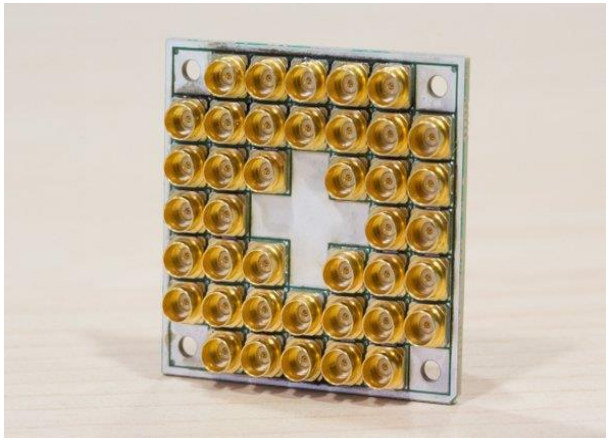
(1) generating ququard-entanglement; (2) preparing initial single-qubit states; (3) implementing single-qubit operations; (4) realizing linear-combination; (5) performing measurement.

Xiaogang Qiang, Xiaoqi Zhou, Jianwei Wang, Callum M. Wilkes, & al., "Large-scale silicon quantum photonics implementing arbitrary two-qubit processing", Nature Photonics, volume 12, pp. 534–539 , 2018

how close are we to build a quantum computer ?



The chips inside IBM's quantum computer (at bottom) are cooled to 15 millikelvin. Near the 50-qubit milestone.



Intel has created 49 qubit- and 17 qubit (shown here) superconducting test chips for quantum computing.

quantum simulation machines