A Basic Introduction to Quantum Computing: hardware, software, and applications

Larry S. Liebovitch
people.qc.cuny.edu/faculty/Larry.Liebovitch/

Departments of Physics & Psychology
Queens College, City University of New York
Physics Program
The Graduate Center, City University of New York

Adjunct Senior Research Scholar
Advanced Consortium on Cooperation, Conflict, and Complexity at
The Earth Institute at Columbia University in the City of New York

Larry S. Liebovitch

Teaching

Hardware & Algorithms of Quantum Computing

CUNY Graduate Center, Jan. 31, 2020, Fridays 2:00 – 4:00 PM
access at: people.qc.cuny.edu/faculty/Larry.Liebovitch/

Courses:

Astronomy, Complex Systems, Mathematics, Physics, Psychology

YouTube:

Statistics: *Methods in Complex Systems*
Computer Science: *Smart Physics for Brilliant Computer Engineers – Season 2*

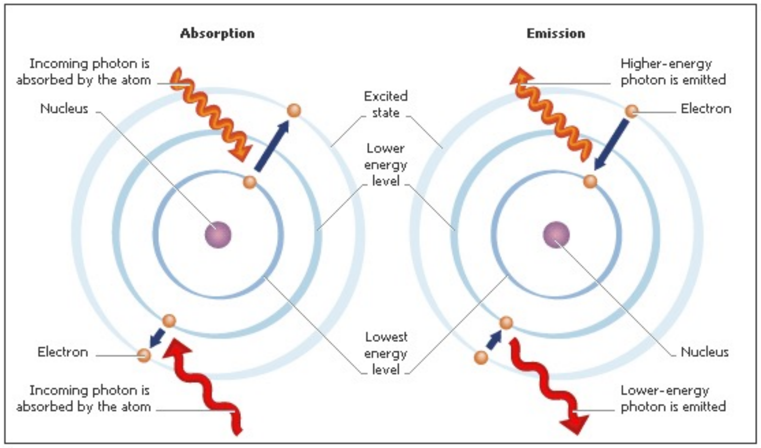
Research

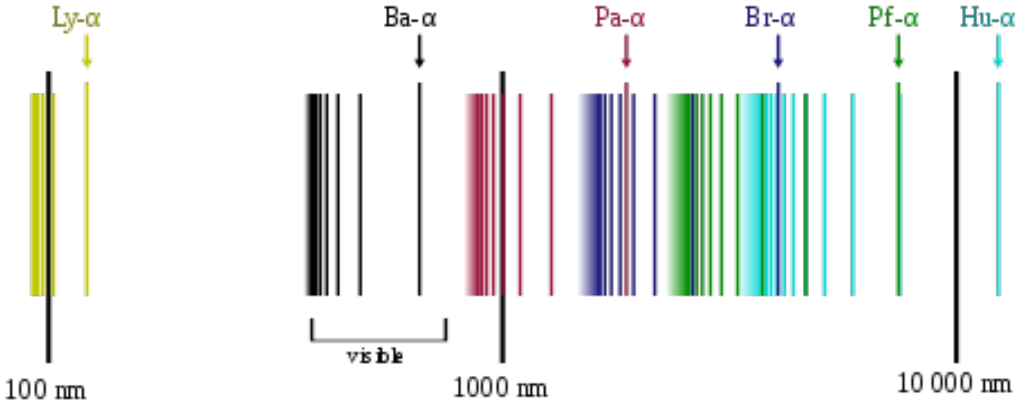
Mathematical Models & Data Science of Complex Systems

motion of stars and gas in galaxies
gene regulatory networks
conditions needed for sustainable peace in the world

Quantum Predicts/Explains

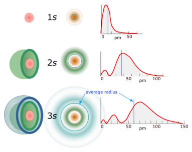
Spectra



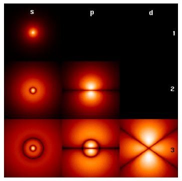


Chemistry

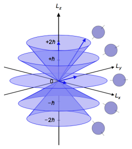
n = principle quantum number
distance of the electron from the nucleus



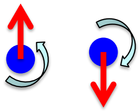
ℓ = angular momentum
how non-circular is the electron orbit around the nucleus

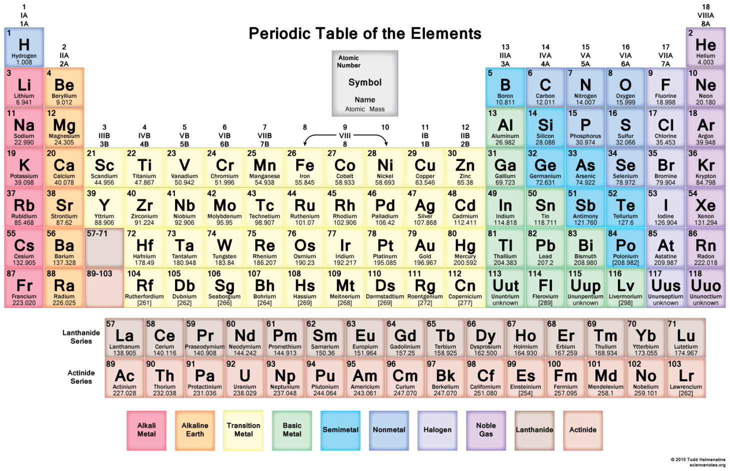


m_ℓ = azimuthal quantum number
how tipped up/down is the electron orbit



m_s = spin of the electron





Periodic Table of the Elements

Alkali Metal	Alkaline Earth	Transition Metal	Basic Metal	Semimetal	Nonmetal	Halogen	Noble Gas	Lanthanide	Actinide

https://en.wikipedia.org/wiki/Hydrogen_spectral_series
http://www.bariblock.eu/protezione-dalle-radiazioni/
http://sciencenotes.org/hd-periodic-table-wallpaper-muted-colors-2015//

Quantum Theory

SUCCESES

- Spectra
- Periodic Table
- Radioactivity
- Transistors
- Superconductivity
- Many others

FAILURES

- Gravity
  - no quantum gravity
- Molecules
  - cannot compute or predict structures, dynamics

Quantum Computers

Richard Feynman (1970s)
If complex quantum systems are hard to compute by conventional computers, use quantum computers to compute them.

Rationale for Quantum Computers

If we can get Quantum Computers to compute COMPLEX quantum systems.

We can use those Quantum Computers to compute MANY other equally COMPLEX systems.

cryptography
finance
weather
biology
social systems

Is it true?

Quantum Computers

BIG Companies

- **Google**
- **IBM**
- **Microsoft**
- **Amazon**
- **Intel**
- Alibaba Group
- Baidu
- Goldman Sachs
- Huawei
- J. P. Morgan Chase

Startups

- D-Wave Systems
- IonQ
- Regetti
- Qrypt
- Tunnel
- Quantum Circuits
- Xanadu

100+ other Companies

https://quantumcomputingreport.com/players/

“Quantum Supremecy”

Quantum Computers

could be 10^{28} times faster then current computers
10,000,000,000,000,000,000,000,000,000

VERY DIFFERENT hardware: NO more bits, RAM, HD, SSD
VERY DIFFERENT software: NO more C++, Python, FORTRAN .. . . COBOL

Hard Parts

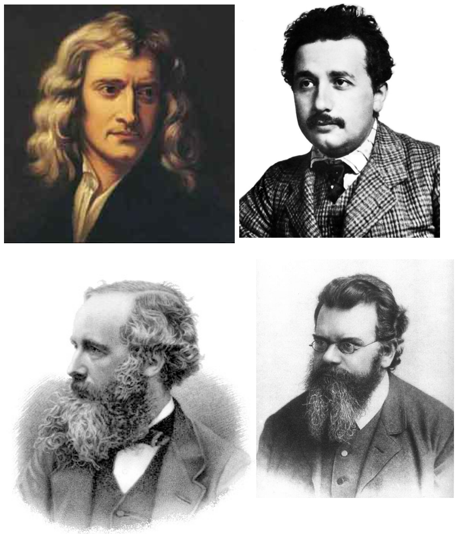
UNDERSTANDING the essential PRINCIPLES of Quantum Mechanics that set the design features of

- hardware
- software

Getting the HARDWARE to work without (too many) errors

Creating the SOFTWARE ALGORITHMS that solve real-world problems

Different Worlds - Different Behaviors



Izzy, Al, Jimmy, Ludva

Everyday Physics

everyday world: **BIG** things
motions, forces, gravity, heat
deterministic
measure and predict with certainty

Marie, Niels, Erwin, Paul

Quantum Mechanics

hidden world: **smallest** things
light (photons), atoms, transistors
probabilities
you measure it, you change it

Quantum "Copenhagen Interpretation"

1. **BEFORE** you measure there are **MANY** possibilities.

2. **WHEN** you measure you find only **ONE** result.
   "the wave function 'collapses' to the measurement"

3. You can predict **ONLY** the **PROBABILITY** of a result.

4. In a Quantum Computer the things you measure are called **Qubits.**

ONE Qubit

1. **BEFORE** you measure
   Qubits are **BOTH** [0] and [1], "superposition"

2. **AFTER** you measure
   The Qubits **ONLY** are either a "0" or "1".

3. **ONCE** you measure, can **NEVER** go on computing

4. **CANNOT** make copies before to cheat
   "no-cloning theorem"
   *math: if $O(\psi) = \psi + \psi$, **quadratic in [0],[1] only LINEAR allowed***
   *physics: if $O(\psi) = \psi + \psi$, **x from some, p from others,** Heisenberg!*

Bits vs. Qubits

Classical computer

operations can be irreversible

c = XOR(a,b), can't get a or b back

Quantum Computer

ALL the operations are reversible and unitary

Bits vs. Qubits

Classical computer

bits are **ONLY** 0 or 1.

Quantum Computer

superposition

Qubits are both [0] and [1] at the same time

More computing power than your computer

Many Bits *vs.* *Many Qubits*

Classical computer

n bits

define a **2n** dimensional space

n = 100, **2n = 200**

Quantum Computer

n Qubits

define a $\mathbf{2^n}$ dimensional space

n = 100,

$\mathbf{2^n = 1{,}267{,}650{,}000{,}000{,}000{,}000{,}000{,}000{,}000{,}000}$

Just a few Qubits form a much BIGGER space to work in

Nonillion

Importance of Dimensionality

Plenty of Room at the Top

ALL 7.5 billion people in the world:

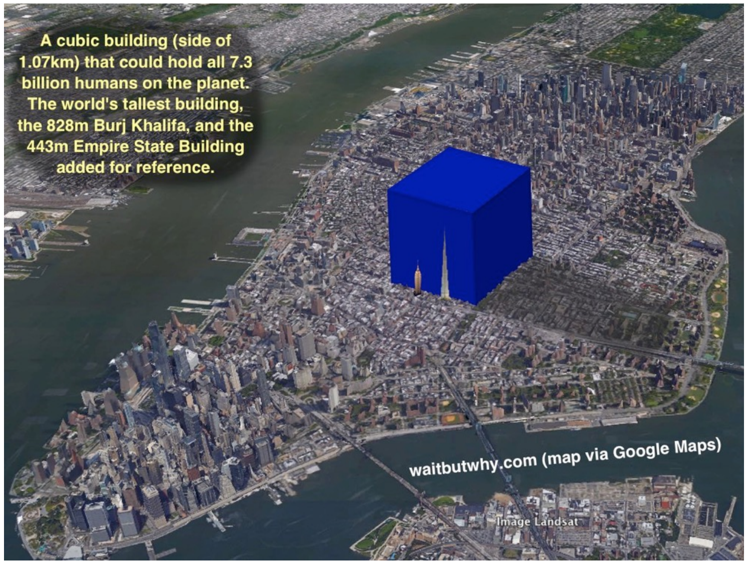
r^1: 1-D line 4,000,000 km

r^2: 2-D area 43 km x 43 km

r^3: 3-D volume 2 km x 2 km x 2 km

waitbutwhy.com

https://waitbutwhy.com/2015/03/7-3-billion-people-one-building.html



A cubic building (side of 1.07km) that could hold all 7.3 billion humans on the planet. The world's tallest building, the 828m Burj Khalifa, and the 443m Empire State Building added for reference.

waitbutwhy.com (map via Google Maps)

Bits vs. *Qubits*

Classical computer

You can **know** the computation values at each step
You get a **definite answer** to your computation

Quantum Computer

You **can't know** the intermediate values in the computation (that would collapse the wave function)
ONLY get the **probability** of the correct **answer**

Bits vs. Qubits

Classical computer

Most Complex:
BPP (Bounded-error Probabilistic Polynomial)

Quantum Computer

Most Complex:
BQP (Bounded-error Quantum Polynomial)
thought that BQP > BPP.

"Quantum Supremacy"

HIGH information content

Each Qubit

(∞ digits) *both [0], [1] same time*

HIGH information content

n QUBITS together

high dimension = 2^n

MASSIVELY Parallel (sort of)

ψ samples whole space

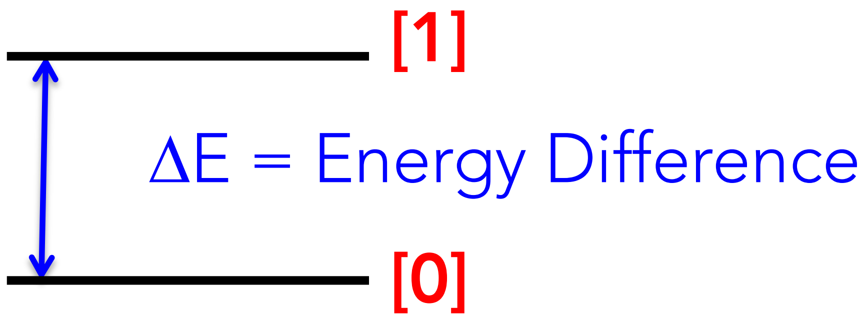
SOLVE more complex problems

BQP > BPP (maybe)

QUANTUM Computer

HARDWARE - Qubits

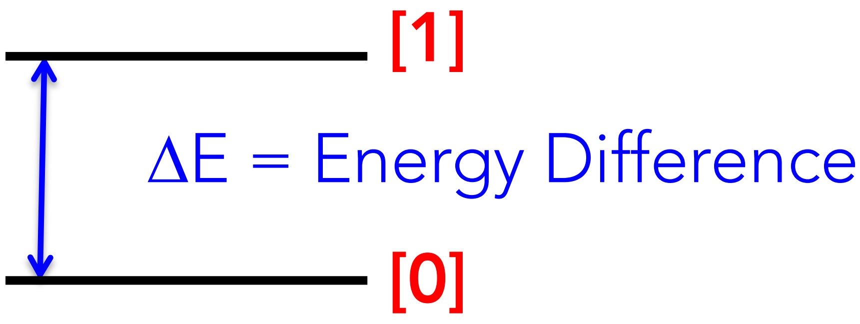
Anything:



QUANTUM Computer

HARDWARE - Qubits

Anything:



[1]

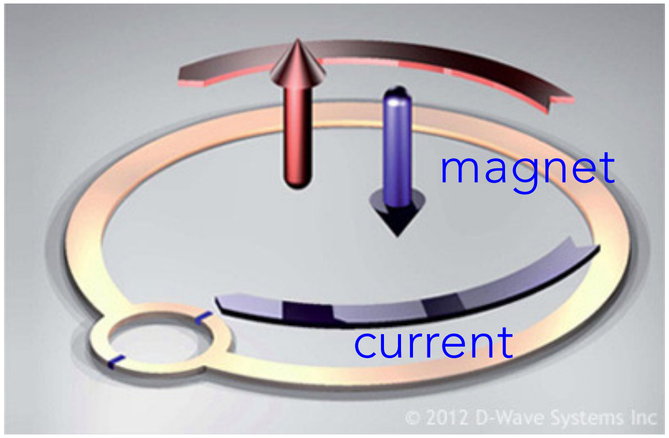
ΔE = Energy Difference

[0]

Anything:

- bits of electricity
- bits of magnetism
- single atoms
- dots of atoms
- wrong atoms in crystals
- light
- positions of things
- shapes of boundaries

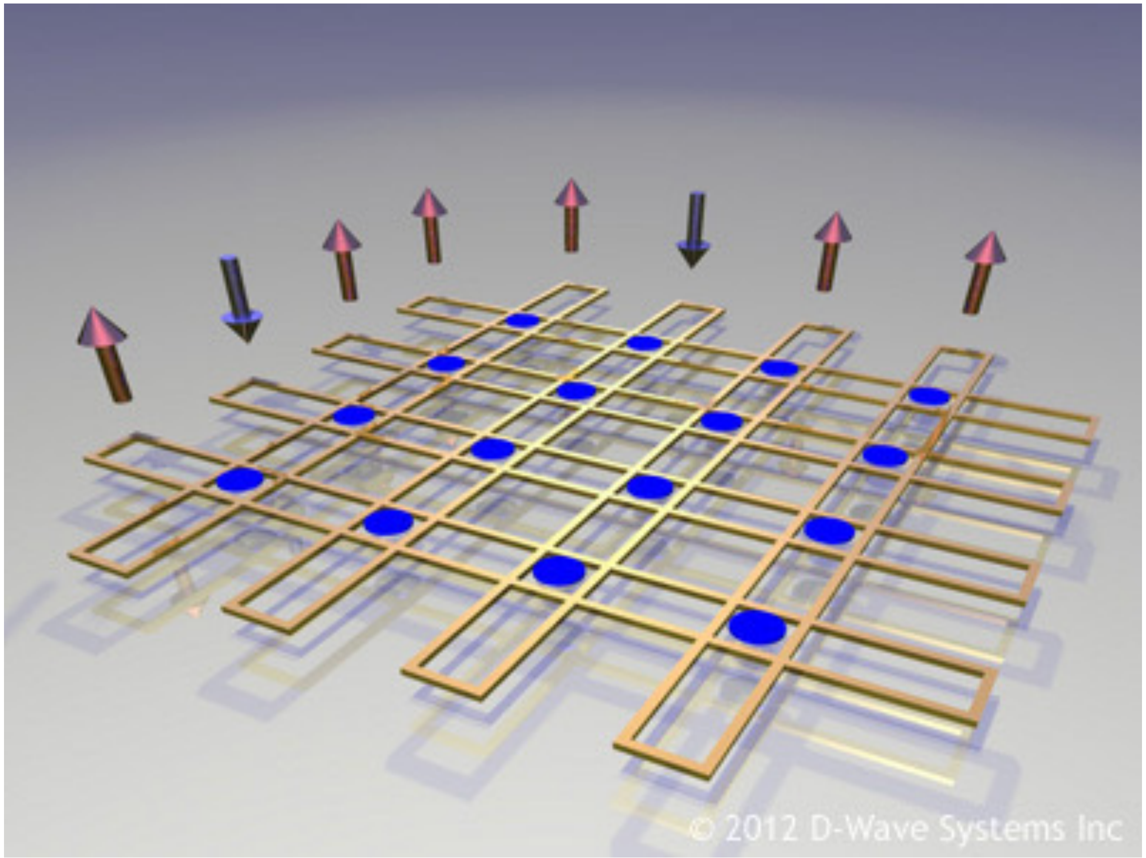
Quantum Computer Hardware
D-Wave Systems



Qubit

Notice: right-hand rule!

Cold: 0.015 K
Shielded: magnetic, radio (emf)

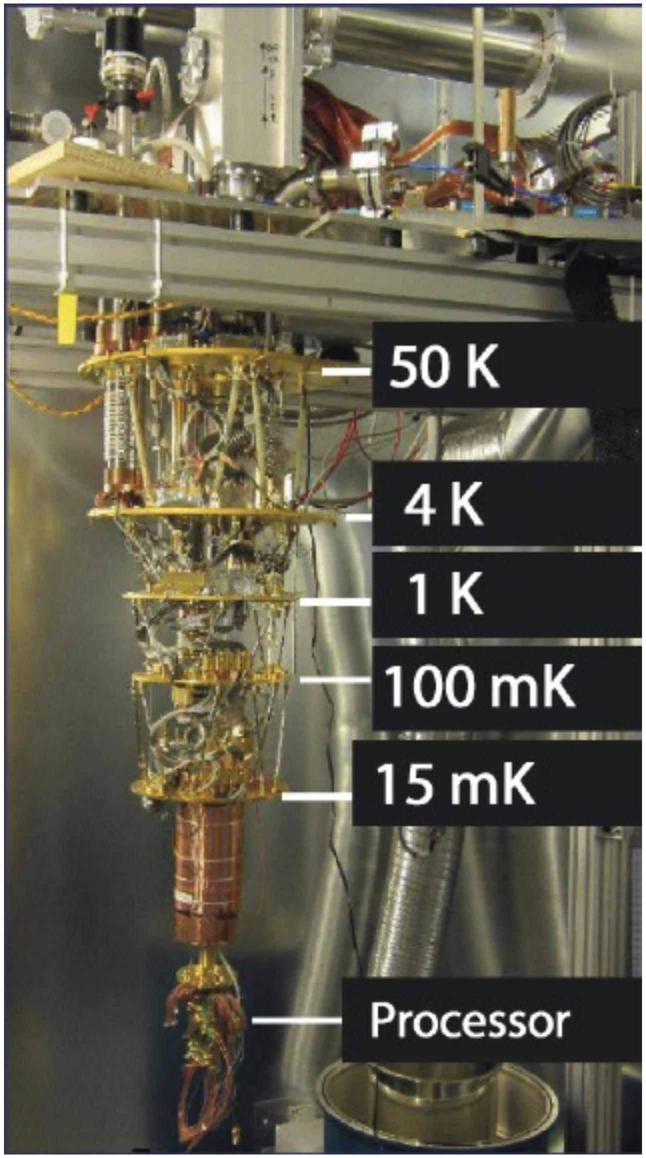


Many Qubits

http://www.dwavesys.com/tutorials/background-reading-series/introduction-d-wave-quantum-hardware

Quantum Computer Hardware

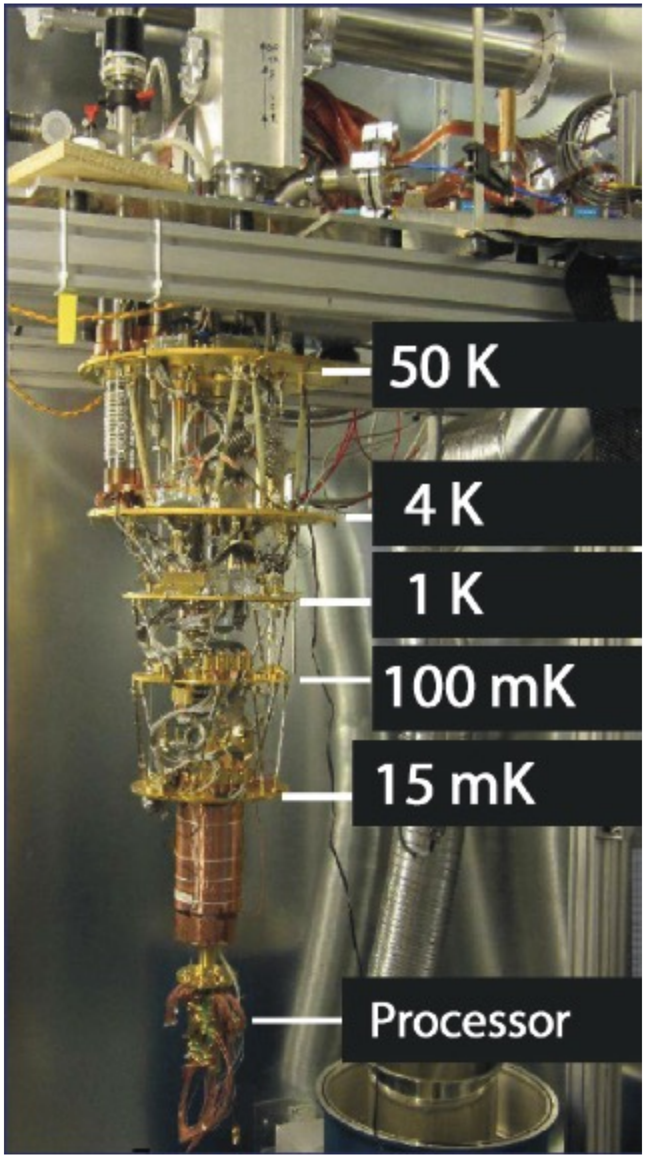
D-Wave Systems



http://www.dwavesys.com/sites/default/files/D-Wave%202X%20Tech%20Collateral_1016F.pdf
http://www.dwavesys.com/resources/media-resources

Quantum Computer Hardware

D-Wave Systems



WHY

So

COLD?

http://www.dwavesys.com/sites/default/files/D-Wave%202X%20Tech%20Collateral_1016F.pdf
http://www.dwavesys.com/resources/media-resources

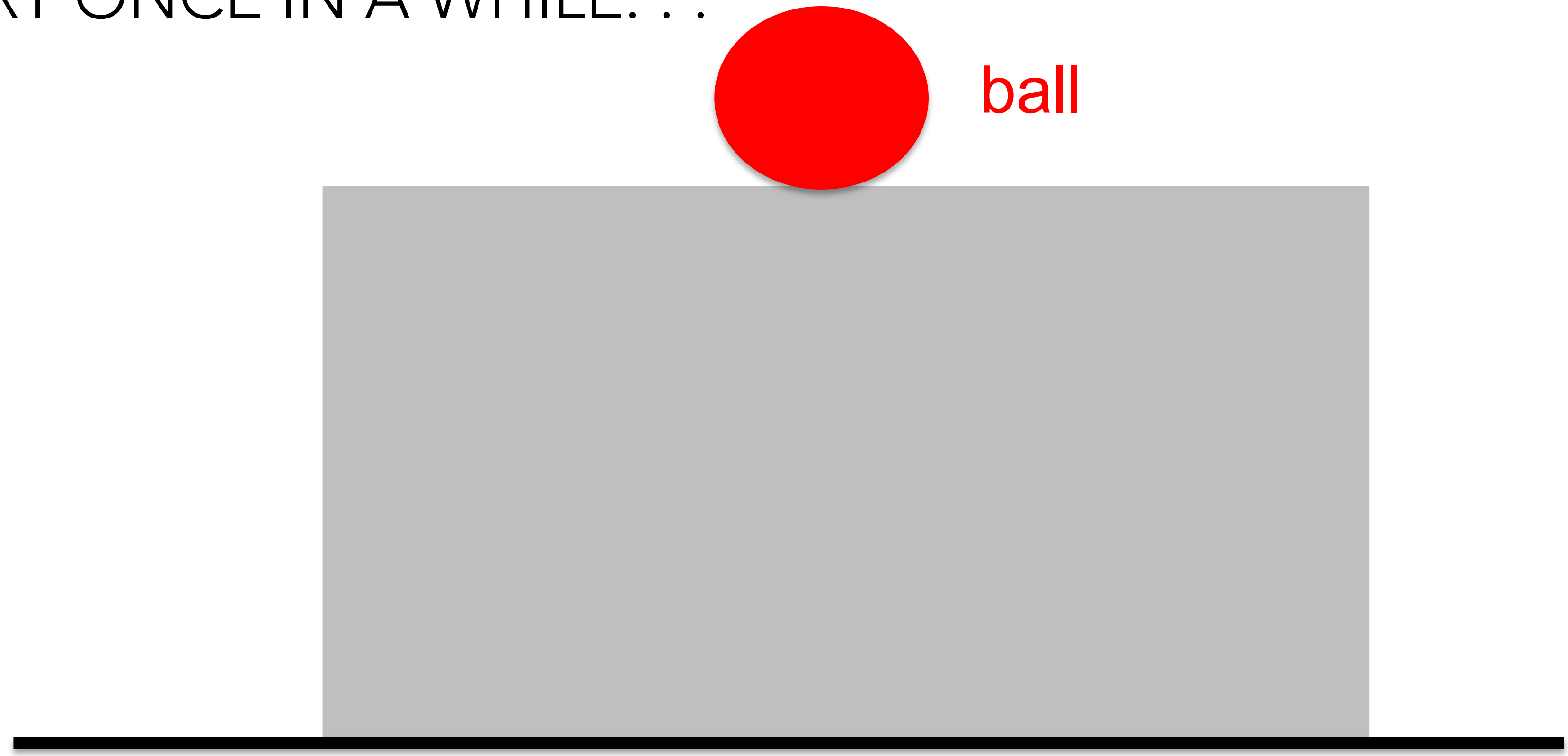
Temperature

Temperature T
At each Temperature ANYTHING has energy

Temperature

Temperature T
At each Temperature ANYTHING has energy

So, EVERY ONCE IN A WHILE. . .



How Often when ΔE BIG?

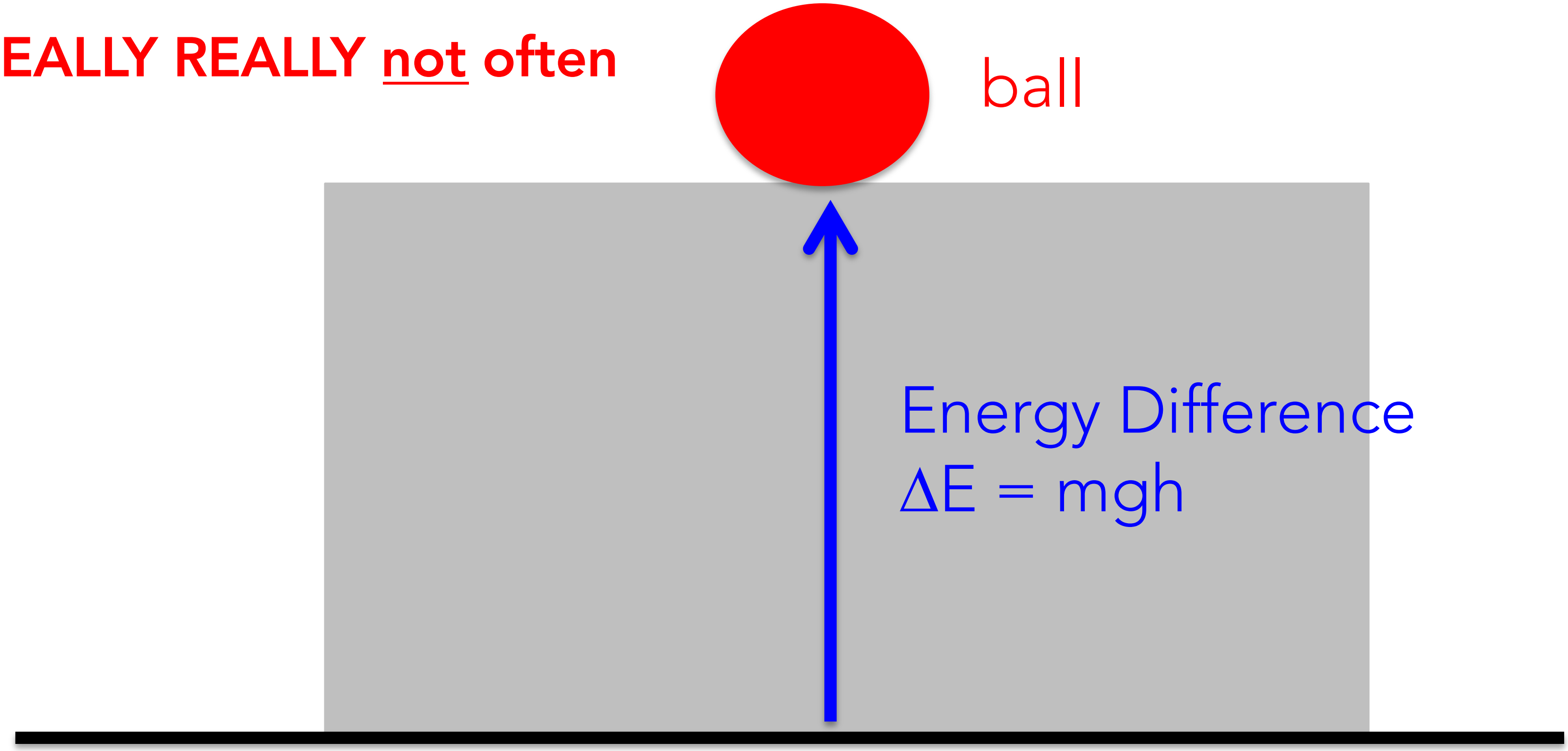
$m = .15$ kg (baseball), $g = 9.8\ \mathrm{ms}^{-2}$, $h = .10$ m,

$T = 293$ K (68 F), $k = 1.38 \times 10^{-23}$ J/K

Time Spent (high) = [$e^{-\Delta E / kT}$] Time Spent (low)

Time Spent (high) = [$10^{-10{,}000{,}000{,}000{,}000{,}000{,}000}$] Time Spent (low)

REALLY REALLY REALLY <u>not</u> often



10,000,000,000,000,000,000 = "ten quintillion"

How COLD D-WAVE?

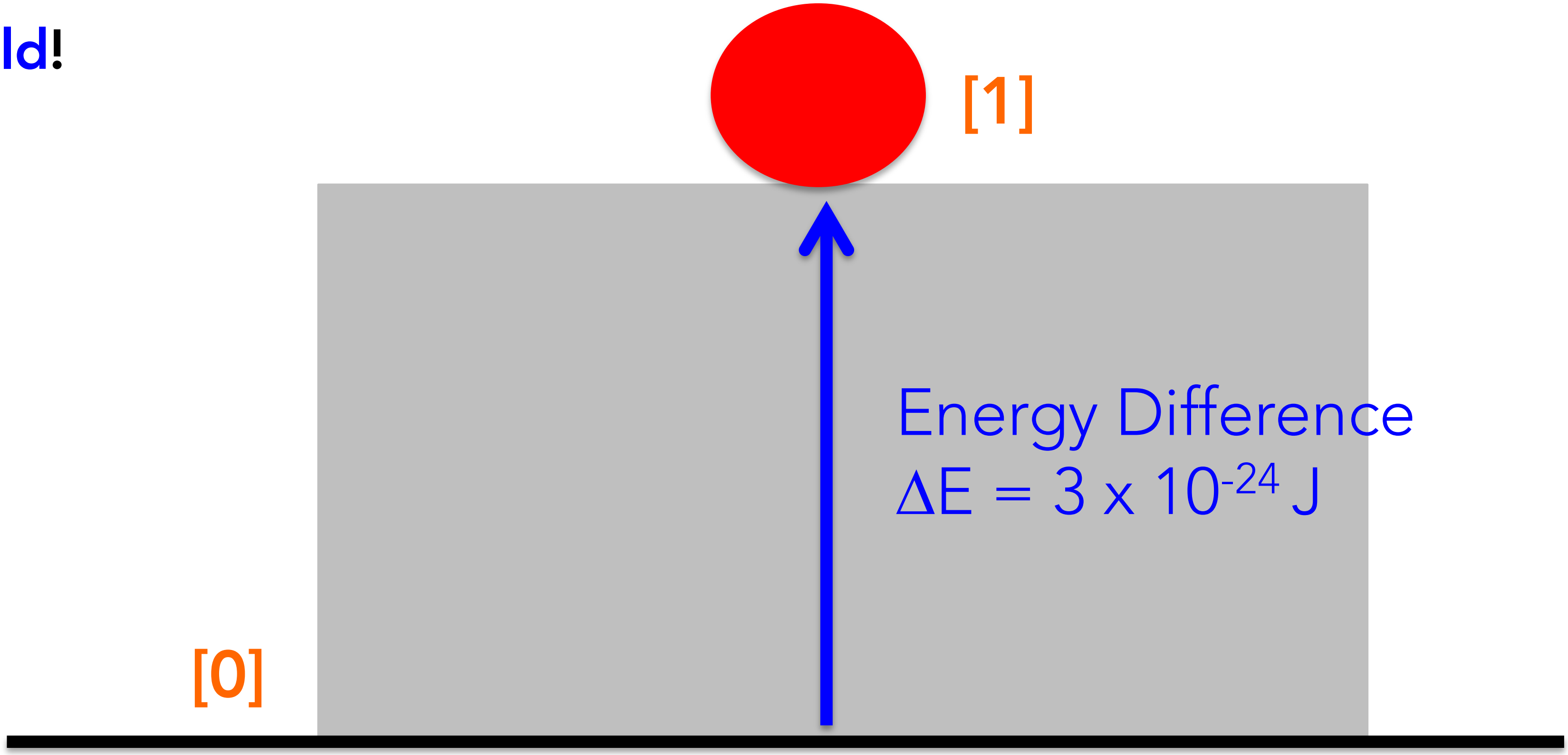
$\Delta E = 3 \times 10^{-24}$ J

$k = 1.38 \times 10^{-23}$ J/K

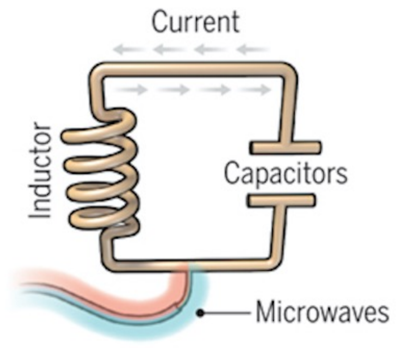
Time Spent (high) / Time Spent (low) = $[e^{-\Delta E / kT})] = 10^{-6}$

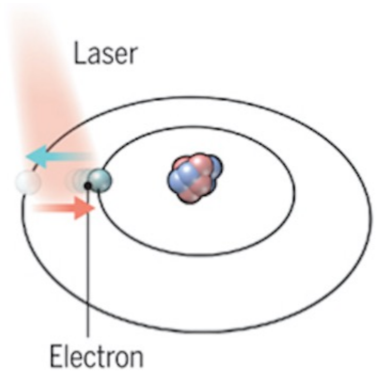
$T = 0.0157$ K = 15 mK

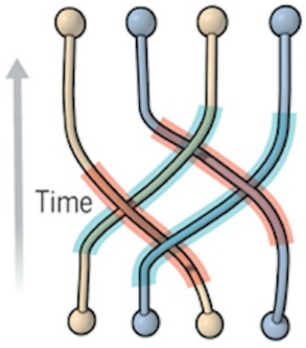
REALLY cold!

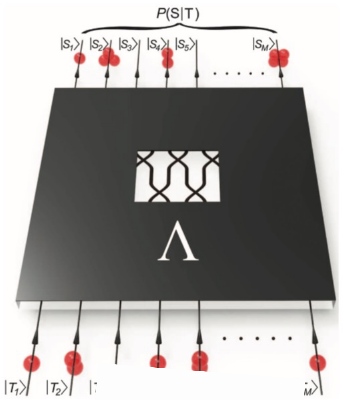


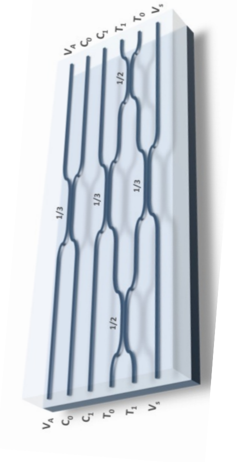
Typical QUBITS











	IC Chips: q, E, B	Isolated Ions	q Positions	Photonics
	Superconducting loops	**Trapped ions**	**Topological qubits**	
	A resistance-free current oscillates back and forth around a circuit loop. An injected microwave signal excites the current into superposition states.	Electrically charged atoms, or ions, have quantum energies that depend on the location of electrons. Tuned lasers cool and trap the ions, and put them in superposition states.	Quasiparticles can be seen in the behavior of electrons channeled through semiconductor structures. Their braided paths can encode quantum information.	
Longevity (seconds)	0.00005	>1000	N/A	
Logic success rate	99.4%	99.9%	N/A	
Number entangled	9	14	N/A	
Company support	Google, IBM, Quantum Circuits	ionQ	Microsoft, Bell Labs	PsiQuantum Tundra Systems
⊕ **Pros**	Fast working. Build on existing semiconductor industry.	Very stable. Highest achieved gate fidelities.	Greatly reduce errors.	
⊖ **Cons**	Collapse easily and must be kept cold.	Slow operation. Many lasers are needed.	Existence not yet confirmed.	

2016 Science 354:1091-1093.
e.sciencemag.org/content/339/6121/798
itation.org/doi/10.1063/1.4976737
rg/pdf/1004.0326.pdf

Wave Functions

Wave Function $\psi = a_1[0] + a_2[1]$

LOOK!: NO bra-kets!

(wave function is solution to the Quantum Mechanic Schrodinger equation).

Superposition: Wave Function is **BOTH** [0] and [1]
and everything in-between until you measure it
WHEN you measure it is **EXACTLY** either [0] or [1]

Born Rule

$|a_1|^2$ = probability of finding state [0] when you measure
$|a_2|^2$ = probability of finding state [1] when you measure

Probability of ALL states = 1

$$|a_1|^2 + |a_2|^2 = 1$$

Quantum Operators MUST BE

UNITARY

$\psi = a_1[0] + a_2[1]$

Born Rule: $|a_1|^2 + |a_2|^2 = 1$

total Probability = 1

REVERSIBLE

math: *Hilbert space:* $u^\dagger u = uu^\dagger = 1$ $(\exists\, u^{-1}\ \forall u)$

physics: Schrodinger Eq:

t -> -t no probability change: $|e^{i\omega t}|^2 = |e^{-i\omega t}|^2$

not dissipative, no entropy

What to do with ONE Qubit

Qubits $[0] = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ $[1] = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

Operations $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \times \begin{bmatrix} e \\ f \end{bmatrix} = \begin{bmatrix} ae + bf \\ ce + df \end{bmatrix}$

X (NOT) $= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

$$\mathbf{X}\,[0] = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = [1]$$

$$\mathbf{X}\,[1] = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = [0]$$

Hadamard

$$[0] = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad [1] = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$\mathbf{H}\ \text{(Hadamard)} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

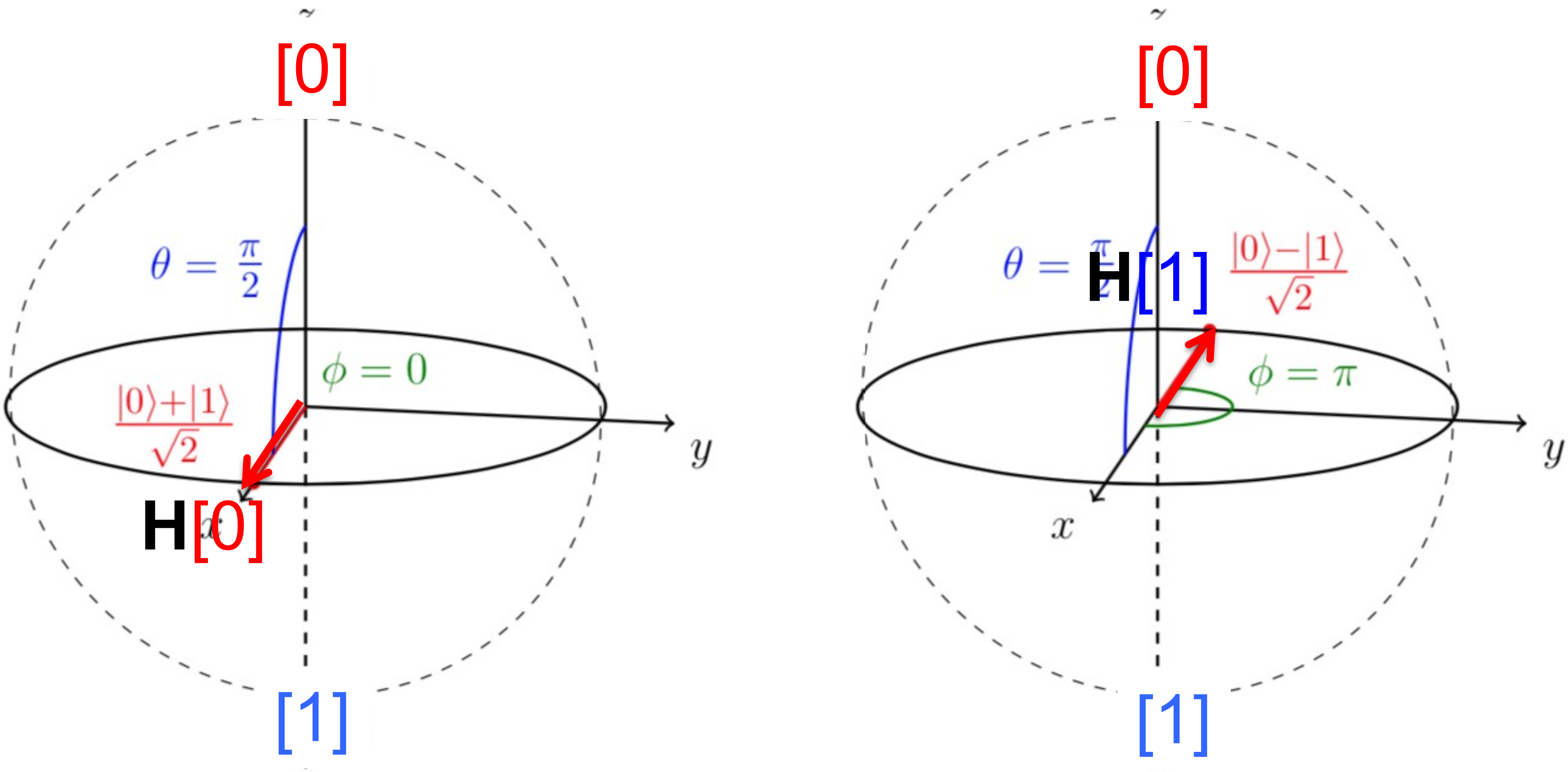
$$\mathbf{H}\ [0] = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \text{ x } \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = 50\%[0] + 50\%[1]$$

$$\mathbf{H}\ [1] = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \text{ x } \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \end{bmatrix} - \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = 50\%[0] + 50\%[1]$$

H converts [0]: to 50% [0] + 50% [1]
H converts [1]: to 50% [0] + 50% [1]

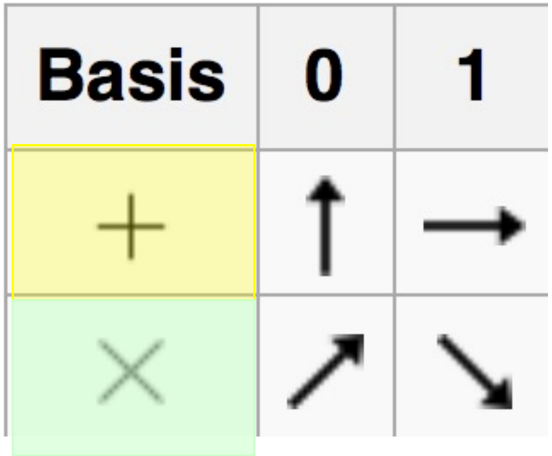
Bloch Sphere

$$\psi = \cos(\theta/2)\ [0] + e^{i\phi} \sin(\theta/2)\ [1]$$



Emma Strubell An Introduction to Quantum Algorithms
http://people.cs.umass.edu/~sturbell/doc/quantum_tutorial.pdf

From ONE BASIS to ANOTHER



Basis	0	1
+	↑	→
×	↗	↘

+ BASIS $[0] = \boxed{\begin{matrix}1\\0\end{matrix}}$ $[1] = \boxed{\begin{matrix}0\\1\end{matrix}}$

x BASIS $=$ **H** (+ BASIS)

$$\mathbf{H} = \text{Hadamard} = \frac{1}{\sqrt{2}}\boxed{\begin{matrix}1 & 1\\ 1 & -1\end{matrix}}$$

+ BASIS	x BASIS
[0] 100%	[0] 50% [1] 50%
[1] 100%	

https://en.wikipedia.org/wiki/Quantum_key_distribution

Quantum Cryptography

100% [0] or [1] *in one BASIS is*
50% [0] & 50% [1] *in another BASIS*

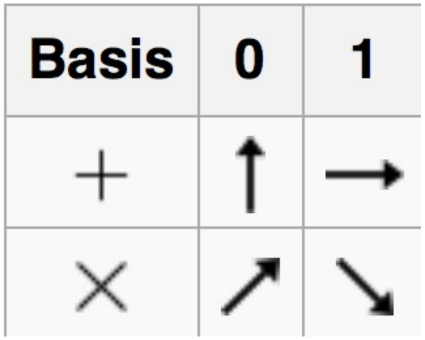
1. SEND A <u>SECURE</u> KEY from one person to another

2. <u>TELL</u> if someone else (an evil actor) was LISTENING IN! NO eavesdropper because measurement changes things

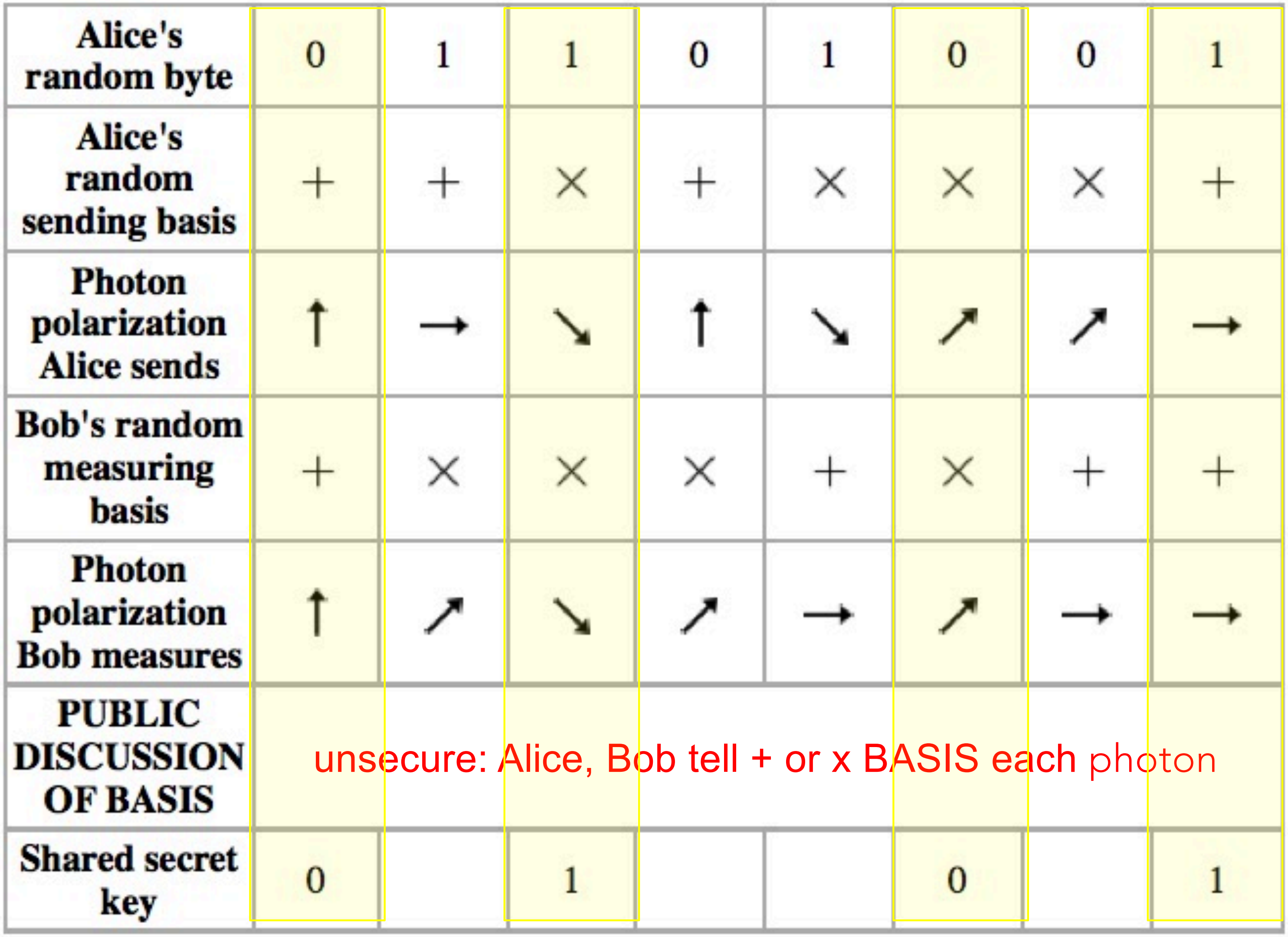
Quantum Key Distribution

BB84 protocol: Charles H. Bennett and Gilles Brassard

if no one is watching



Basis	0	1
+	↑	→
×	↗	↘



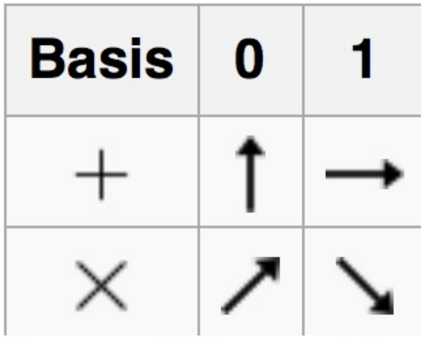
Alice's random byte	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↘	↗	→	↗	→	→
PUBLIC DISCUSSION OF BASIS	unsecure: Alice, Bob tell + or x BASIS each photon							
Shared secret key	0		1			0		1

Alice & Bob DON'T Tell (0,1) ONLY if used + or x BASIS

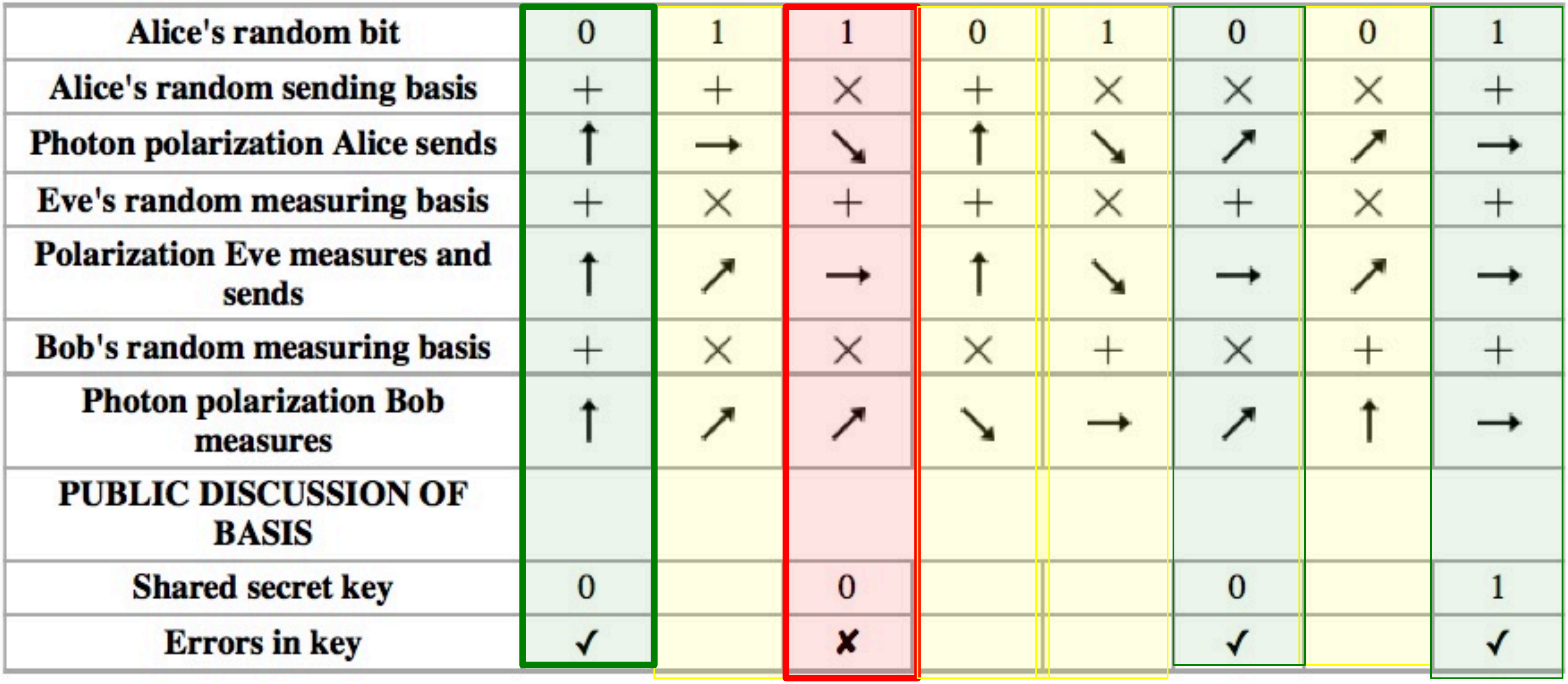
https://en.wikipedia.org/wiki/Quantum_key_distribution

Quantum Key Distribution

if someone is watching!



Basis	0	1
+	↑	→
×	↗	↘



Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Eve's random measuring basis	+	×	+	+	×	+	×	+
Polarization Eve measures and sends	↑	↗	→	↑	↘	→	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↗	↘	→	↗	↑	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		0			0		1
Errors in key	✓		✘			✓		✓

Bob & Alice can TELL if EVE is watching!

¾ of the time Bob gets the WRONG bit, so if insecure compare (waste n = 72 bits). Then P(n) = 1 – $(3/4)^n$ = 0.999999999 NO wrong bits, EVE is not listening.

https://en.wikipedia.org/wiki/Quantum_key_distribution

Quantum Key Distribution networks

DARPA (US)

SECOQC (EU)

SwissQuantum (CH)

China (QUESS satellite)

Tokyo (Japan)

Los Alamos National Laboratory (US)

+ others

What to do with TWO Qubits

$[0] = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad [0] = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

[00] = [0] *x* [0] **TENSOR** product

multiply every piece of **A** by every piece of **B**

dim (A *x* B) = dim (A) x dim(B) = 2 x 2 = 4

(dim (n qubits) = 2^n)

$$[00] = [0] \times [0] = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ 0 \begin{bmatrix} 1 \\ 0 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$[00] = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \qquad [01] = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \qquad [10] = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \qquad [11] = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

2 Qubit Operations

CNOT = CONDITIONAL NOT

leave the first Qubit alone
if the first Qubit =1, switch the second Qubit from (0→1 or 1→0)

CNOT [$a_{in}b_{in}$] = [$a_{out}b_{out}$]

if $a_{in} = 0$: $a_{out} = a_{in}$, $b_{out} = b_{in}$
if $a_{in} = 1$: $a_{out} = a_{in}$, $b_{out} = \mathrm{NOT}(b_{in})$

CNOT [00] = [00]

CNOT [01] = [01]

CNOT [10] = [11]

CNOT [11] = [10]

CNOT

$$\mathbf{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

CNOT operates on 2 Qubits
so it must be dim = 4.

CNOT [ab]
if a=1, change b

$$\mathbf{CNOT\ [00]} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \mathbf{[00]}$$

$$\mathbf{CNOT\ [01]} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \mathbf{[01]}$$

$$\mathbf{CNOT\ [10]} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \mathbf{[11]}$$

$$\mathbf{CNOT\ [11]} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \mathbf{[10]}$$

COMBINE 2 Operations

H *x* 1 = **TENSOR** product

multiply every piece of **H** by every piece of **1**

dim (**H** *x* **1**) = dim (**H**) x dim(1) = 2 x 2 = 4

$$\frac{1}{\sqrt{2}}\boxed{\begin{matrix}1 & 1\\ 1 & -1\end{matrix}}\; x \;\boxed{\begin{matrix}1 & 0\\ 0 & 1\end{matrix}} = \frac{1}{\sqrt{2}}\boxed{\begin{matrix}1\boxed{\begin{matrix}1 & 0\\ 0 & 1\end{matrix}} & 1\boxed{\begin{matrix}1 & 0\\ 0 & 1\end{matrix}}\\ 1\boxed{\begin{matrix}1 & 0\\ 0 & 1\end{matrix}} & -1\boxed{\begin{matrix}1 & 0\\ 0 & 1\end{matrix}}\end{matrix}} = \frac{1}{\sqrt{2}}\boxed{\begin{matrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 1 & 0 & -1 & 0\\ 0 & 1 & 0 & -1\end{matrix}}$$

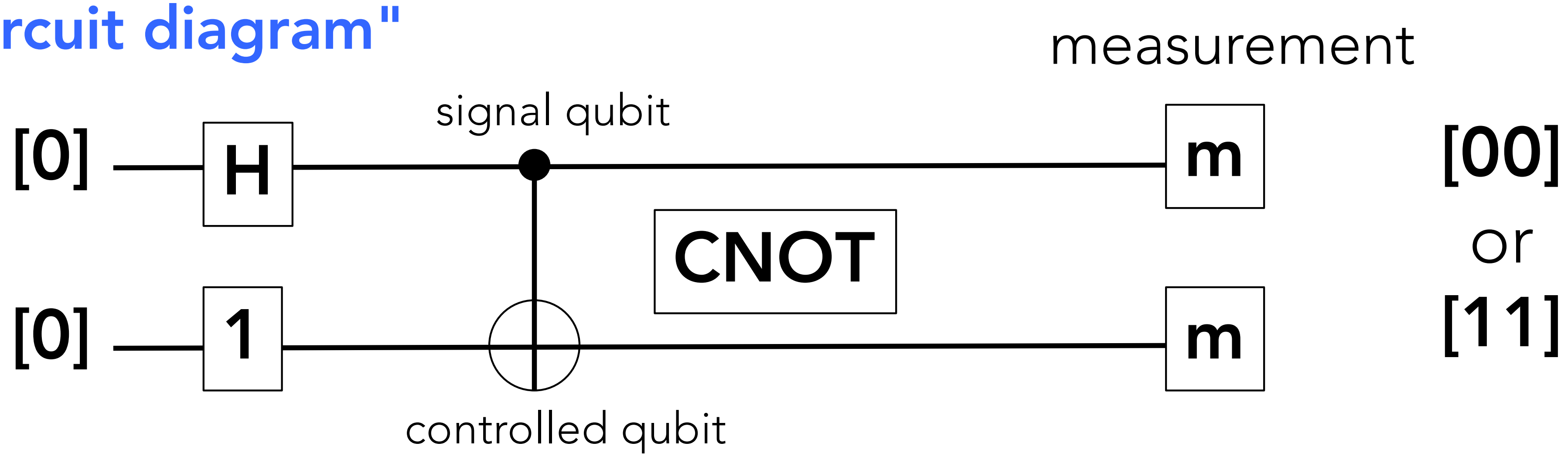
NOW for some fun!

CNOT (H x 1) [00]

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

$$= \frac{1}{\sqrt{2}} [00] + \frac{1}{\sqrt{2}} [11]$$

"circuit diagram"



NOW for some fun!

CNOT (H $\times$ 1) [00]

$$\boxed{\begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{matrix}} \frac{1}{\sqrt{2}} \boxed{\begin{matrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{matrix}} \boxed{\begin{matrix} 1 \\ 0 \\ 0 \\ 0 \end{matrix}} = \boxed{\begin{matrix} 1 \\ 0 \\ 0 \\ 1 \end{matrix}} = \frac{1}{\sqrt{2}} \boxed{\begin{matrix} 1 \\ 0 \\ 0 \\ 0 \end{matrix}} + \frac{1}{\sqrt{2}} \boxed{\begin{matrix} 0 \\ 0 \\ 0 \\ 1 \end{matrix}}$$

$$= \frac{1}{\sqrt{2}} [00] + \frac{1}{\sqrt{2}} [11]$$

50% of the time we measure **[00]**
50% of the time we measure **[11]**

NEVER measure **[01]** or **[10]**

NOW for some fun!

CNOT (H $\times$ 1) [00]

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

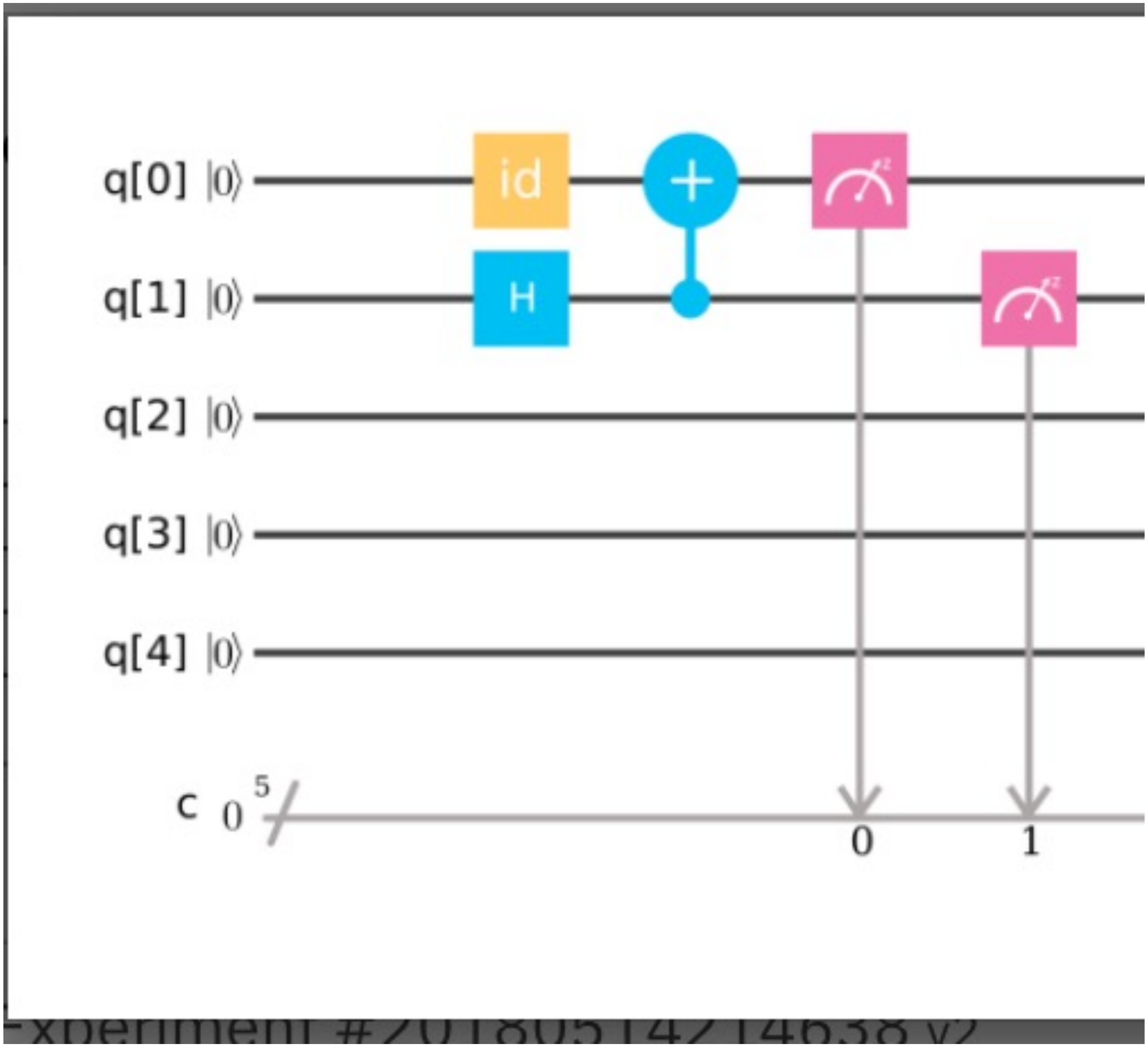
$$= \frac{1}{\sqrt{2}} [00] + \frac{1}{\sqrt{2}} [11]$$

50% of the time we measure **[00]**
50% of the time we measure **[11]**

NEVER measure **[01]** or **[10]**

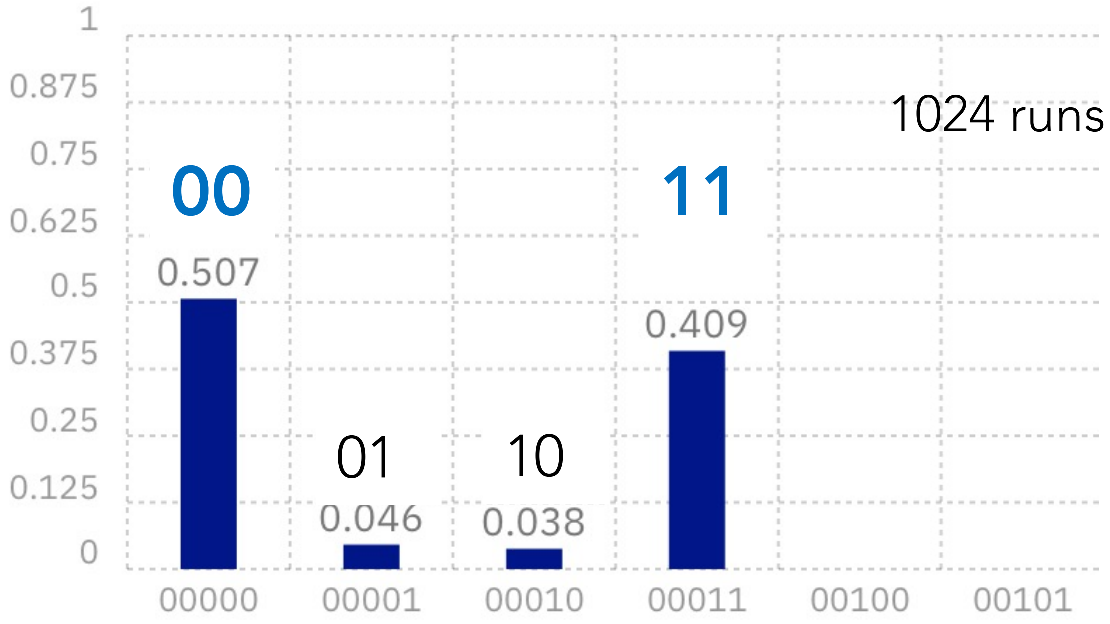
spukhafte Fernwirkung
"spooky action at a distance"
ENTANGLEMENT

IBM: https://quantumexperience.ng.bluemix.net/qx/editor

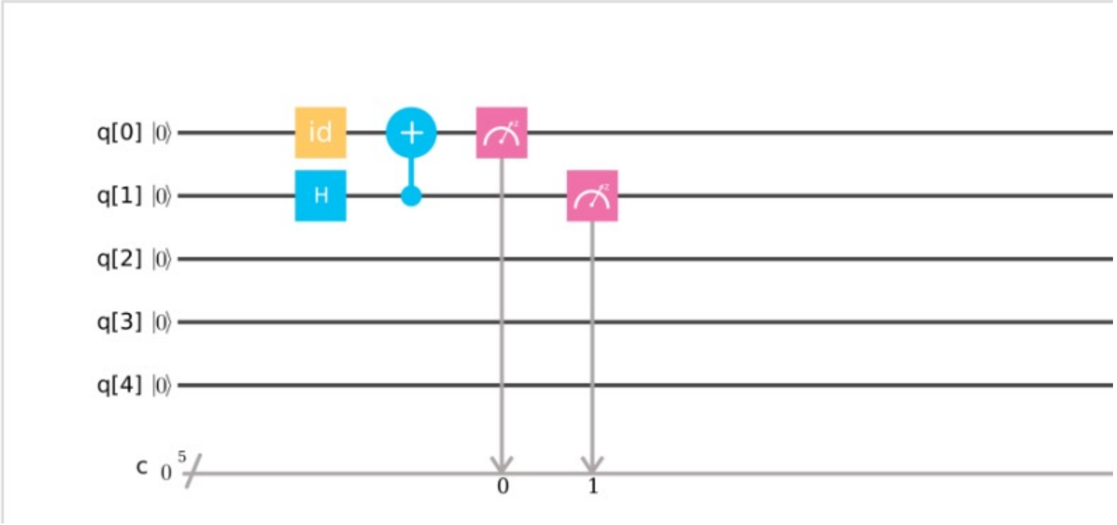


IBM
IBM Q 5
Tenerife
[ibmqx4]

Quantum State: Computation Basis



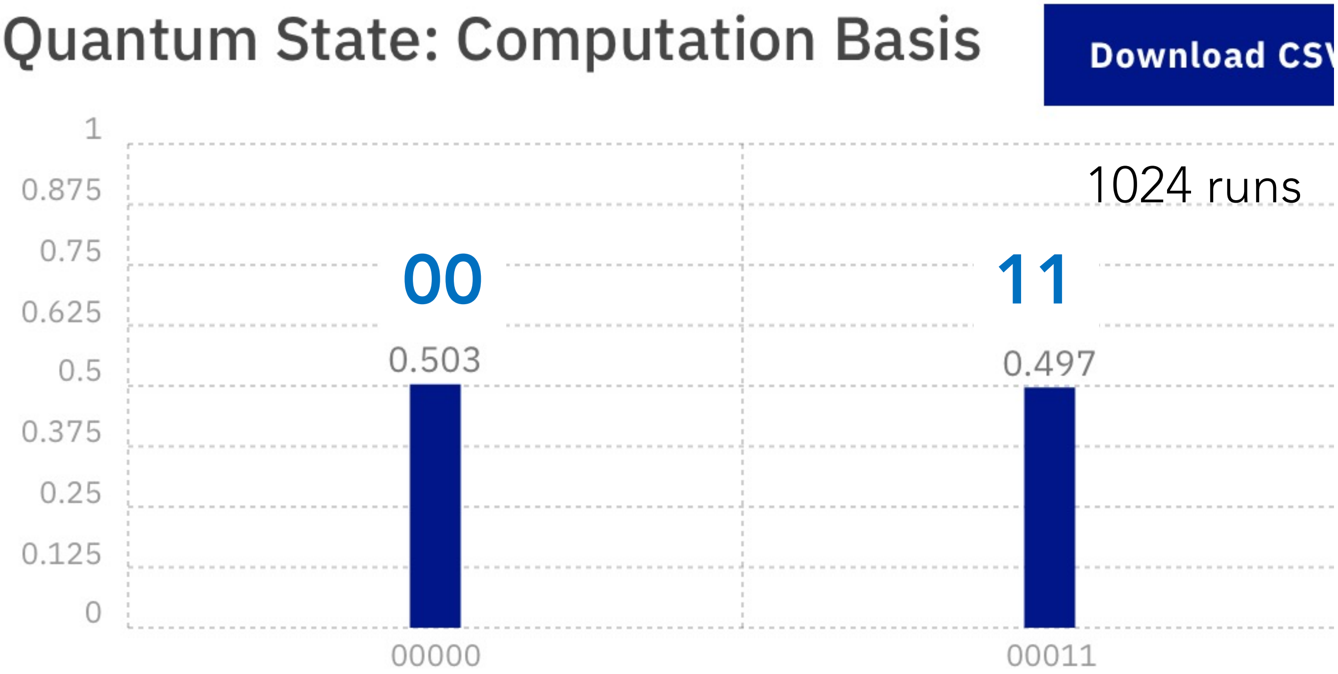
Quantum Circuit



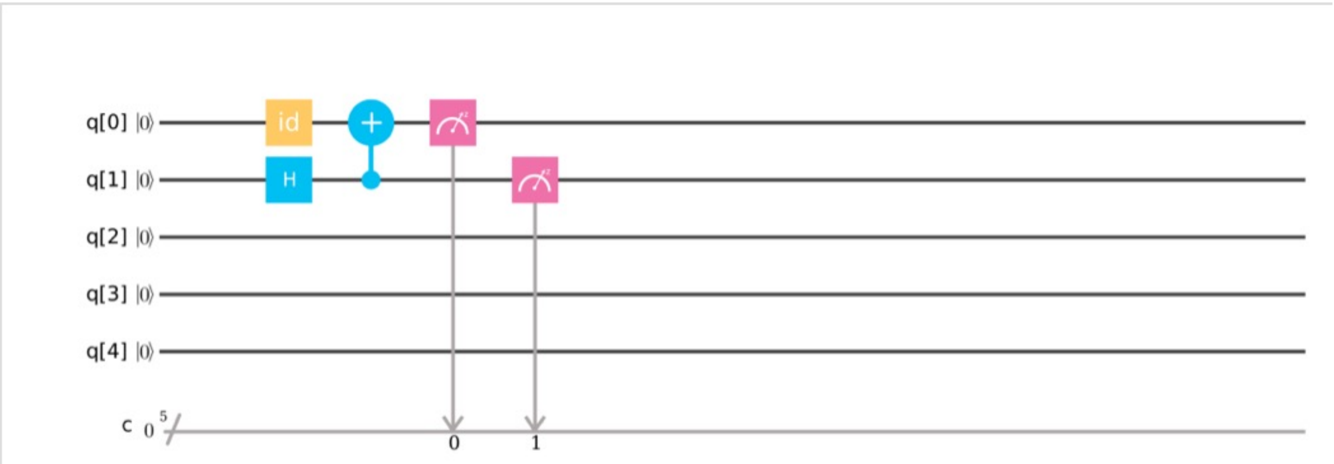
IBM
IBM Q 5
Tenerife
[ibmqx4]

Device: Simulator

Quantum State: Computation Basis



Quantum Circuit

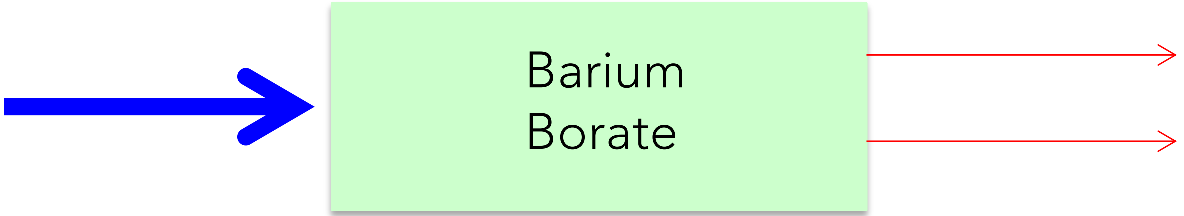


σ = sqrt(npq)
n = 1024
p = q = 0.5
σ = sqrt(256) = 16
16/1024 = 0.016
0.503-0.497=0.006

Making Entangled Photons

Spontaneous Downconversion

http://spookyactionbook.com/2016/02/21/faq-how-are-entangled-particles-created-video/


Barium
Borate

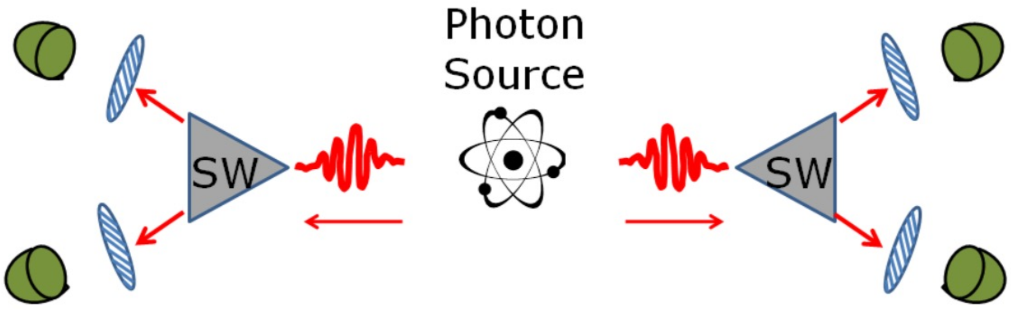
quantum noise

$1:10^9$
Type I: [00]
Type II: [01]

2-Photon Production

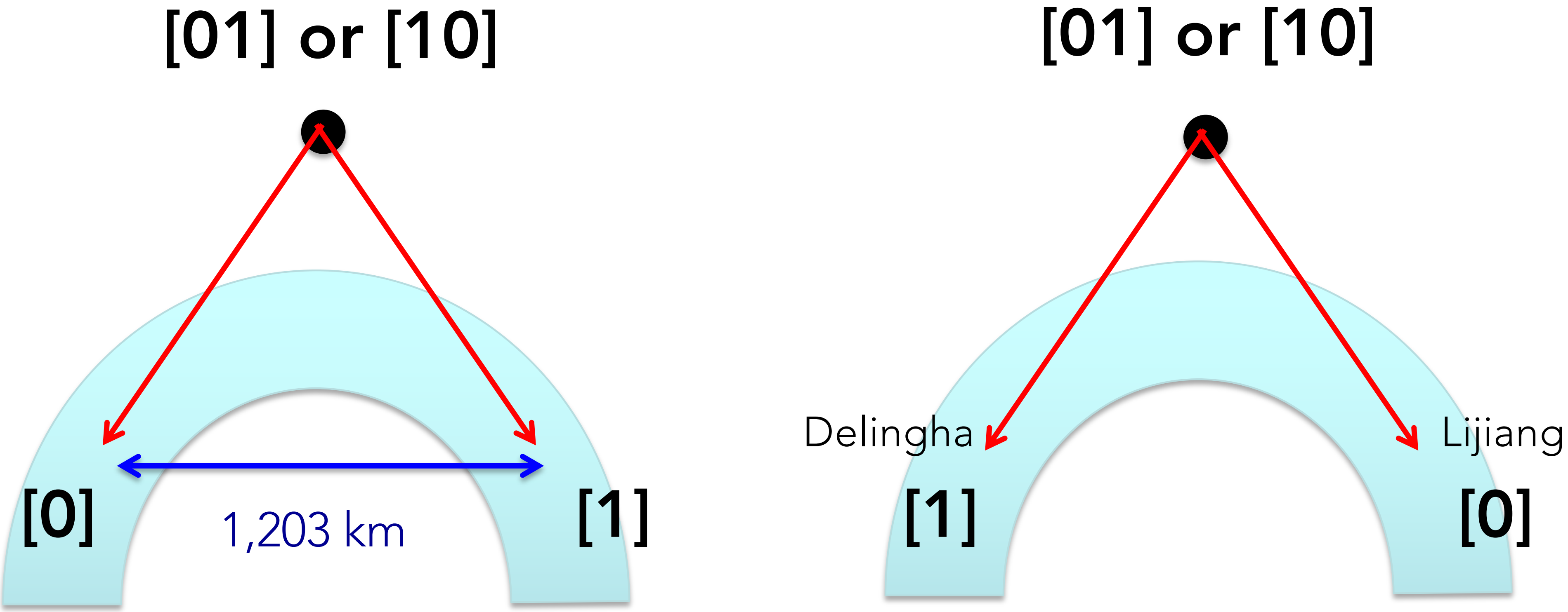
Ca atoms forbidden single photon transition to the ground state

https://www.forbes.com/sites/chadorzel/2017/02/28/how-do-you-create-quantum-entanglement/#529cb121732b



Micius Satellite Entanglement

Yin et al. 2017. Science 356:1140-1144.



ALWAYS [01] or [10] NEVER [00] or [11]
NOT that we measure [0] and it tells the other one to be [1]
NO INFINTELY FAST ACTION AT A DISTANCE!

A continuous-wave laser diode with a central wavelength of 405 nm and a linewidth of ~160 MHz is used to pump a periodically poled KTiOPO4 (PPKTP) crystal inside a Sagnac interferometer. The pump laser, split by a polarizing beam splitter (PBS), passes through the nonlinear crystal in clockwise and anticlockwise direction simultaneously, which produces down-converted photon pairs at ~810 nm wavelength in polarization-entangled states close to the form [01] . . Sending: .two Cassegrain telescopes 18 and 30 cm . . Receiving:China: Delingha and Lijiang, 120 and 180 cm

Public Key Encryption – RSA

Alice sends a public key to Bob
Bob uses that key to send a message to Alice
that ONLY Alice can read.

n = p x q

if someone else can factor n into p and q
they can read Bob's message!

Public Key Encription – RSA in pictures

Alice sends the public keys to Bob
Bob will use them to send a message back to Alice
that ONLY Alice can read.

Alice

choses p, q
p, q -> n, e, d

sends n, e to Bob
keeps d secret

decrypts c
$c^d = (m^e)^d = m^{ed} = m^1$
mod (n)

green = open
ANYONE can see

n,e

c

Bob

message = m

uses n,e to
encrypt m as
$c = m^e \bmod (n)$

sends c to Alice

Factoring Algorithms

Factoring the n of RSA-2048

n = 2048 binary digits

Classical Computer

number of operations

= 10^{38}

$$e^{7\sqrt[3]{n}}$$

Quantum Computer

Shor's algorithm

= 10^{10}

$$n^3$$

Quantum Computer is 10^{28} times FASTER!

https://en.wikipedia.org/wiki/RSA_Factoring_Challenge

Shor's Algorithm to break RSA

1994

long before hardware available

Non-Quantum Part

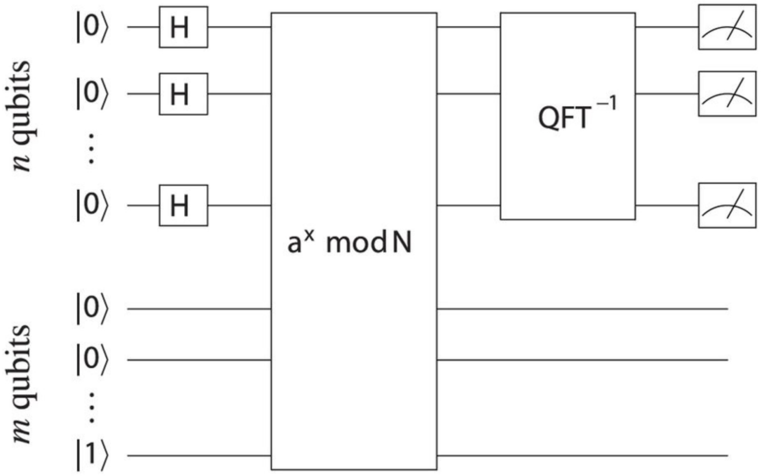
pick a < n

find the period of $f(x) = a^x \bmod n$

Quantum Part

use Quantum Fourier Transforms

to find the period r of $f(a) = a^x \bmod n$



Finding r is

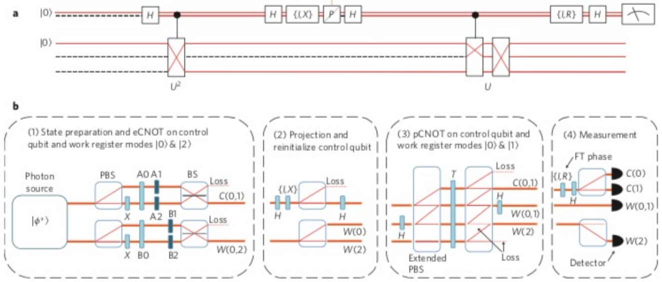
equivalent to factoring n = p x q.

https://en.wikipedia.org/wiki/Shors_algorithm

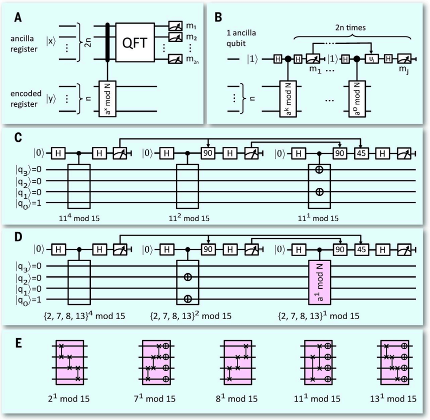
Mermin. 2007. Quantum Computer Science (Cambridge Univ. Press)

Shor's Algorithm – Some Implementations

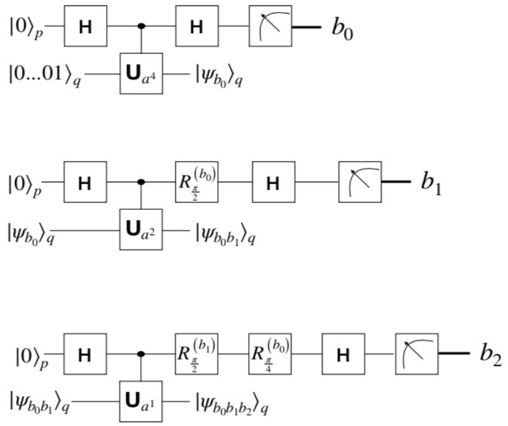
Martın-Lopez et al. 2012
21 = 3 x 7
Nature Photonics
https://www.nature.com/articles/nphoton.2012.259.pdf
photonics: calcite beam displacers and interferometers



Monz et al. 2016
15 = 3 x 5
Science 351:1068-1070
https://science.sciencemag.org/content/351/6277/1068
ion-trap with five Ca+ ions



Amico et al. 2019
15 = 3 x 5
https://arxiv.org/abs/1903.0076
16 superconducting qubits ibmqx5



Deutsch's Algorithm

http://www.cs.xu.edu/~kinne/quantum/deutche.html
https://physics.stackexchange.com/questions/3390/can-anybody-provide-a-simple-example-of-a-quantum-computer-algorithm

Input -> Output

(x,y) -> (x',y')   where x, y, x', y' = (0,1)

Task

f(0) = f(1) SAME output for DIFFERENT inputs INDEPENDENT
f(0) ≠ f(1) DIFFERENT output for DIFFERENT inputs DEPENDENT

Classical Computer

TWO operations: to tell if **INDEPENDENT** vs. **DEPENDENT**

Quantum Computer:

ONE operation can tell if **INDEPENDENT** vs. **DEPENDENT**

but it cannot tell
independent: whether f(0)=f(1)=0 *or* f(0)=f(1)=1
dependent: whether f(0)=0, f(1)=1 *or* f(0)=1, f(1)=0

Deutsch-Jozsa Algorithm

https://en.wikipedia.org/wiki/Deutsch–Jozsa_algorithm

Input: (x_1,y_1) (x_2,y_2) (x_2,y_2) . . . (x_n,y_n)

n (x_i,y_i) pairs of inputs that are 0, 1

Output: (x',y')

1 pair (x',y') where $x' = 0,1$; $y' = 0,1$

Task

SAME output for ALL inputs **INDEPENDENT**

DIFFERENT output for DIFFERENT inputs **DEPENDENT**

Classical Computer

$2^{n-1} + 1$ operations

Quantum Computer:

<u>ONE</u> operation

Grover's Algorithm

Database with n data elements

$n = 10^{10}$

Classical Computer

number of operations n

$= 10^{10}$

Quantum Computer

Grover's algorithm $n^{1/2}$

$= 10^5$

Quantum Computer is 10^5 times FASTER!

https://en.wikipedia.org/wiki/RSA_Factoring_Challenge

REALITY CHECK

Shor’s Algorithm

Already Post-Quantum Cryptography Companies designing quantum resistent encryption

Qrypt, CryptoNext, QuBalt, . . .

Deutsch-Jorzsa Algorithm & Others

Nice "toy" problem, real world applications?

Grover’s Algorithm

Real data is really unordered

hash functions: Blockchain (Bitcoin and elsewhere)

biological systems: “content addressable” O(n=1)

Shor, Deutsch, Grover Algorithms & Feynman, Deustch, Simon, & others TREMENDOUSLY IMPORTANT

That WORK (40 years ago) has NOW led to

REAL quantum computers and REAL algorithms.

Basic research created NEW, unexpected, valuable

possibilities for the REAL WORLD.

When Does Quantum Computing Happen?

It's Already Happened!

- Quantum Computer ECOSYSTEM
    - lots lots $$$ China >> US >> EU
    - creating new chips, solid state, photonics
    - creating new algorithms: find min, machine learning

The importance of DOD cold war spending and the moon landing wasn't landing on the moon, it was: IC chips CPUs, DRAM, HD, LCDs, Li-ion batteries, DSP, HTTP, HTML, GPS, touch screens, AI (M. Mazzucato).

If Quantum Computers Do Happen

- Feynman: quantum systems: molecules, drugs
- high dimensional: physics, chem, bio, psych, social
- science: weather, metamaterials,
- organizations: logistics, social patterns
- finance: fintech

What Happens Next?

> “It’s tough to make predictions,
> especially about the future.”
>
> -Lawrence Peter “Yogi” Berra