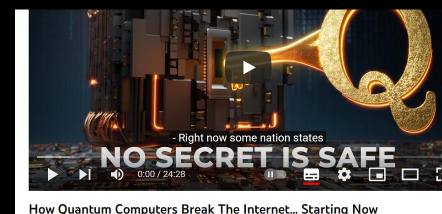
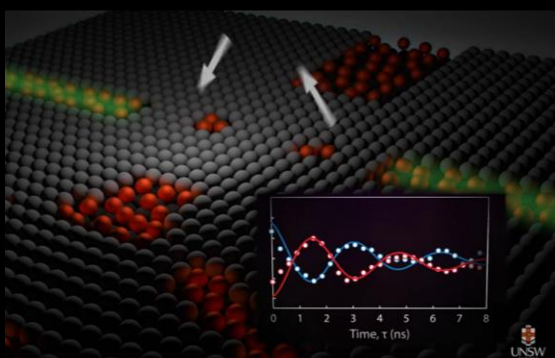
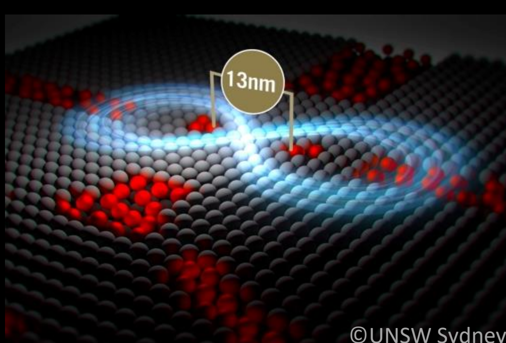
The emergence of quantum computing
Principles, implementations, challenges

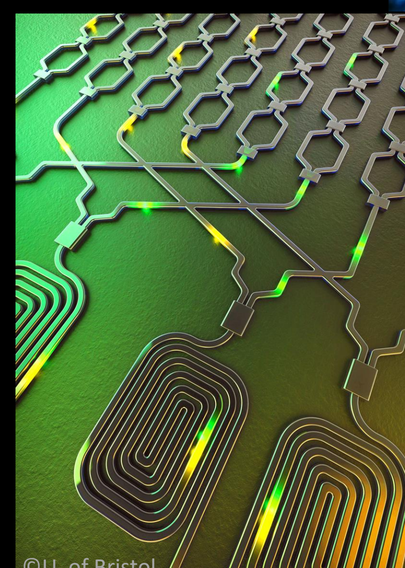
Nadia Belabas @ Goss group http://quantumdot.eu

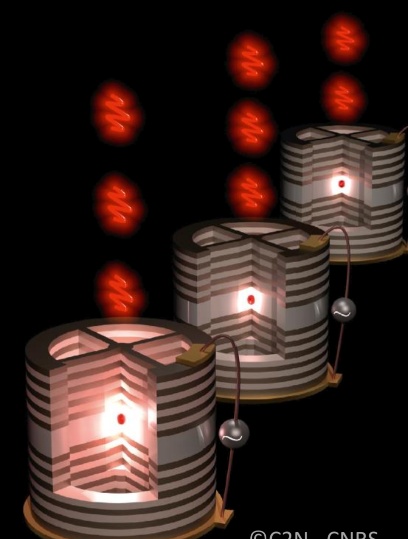
Center for Nanoscience and Nanotechnology C2N
*CNRS – **University** Paris Saclay*







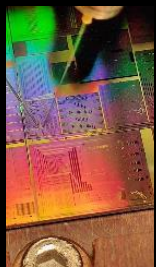




The emergence of quantum computing
Principles, implementations, challenges

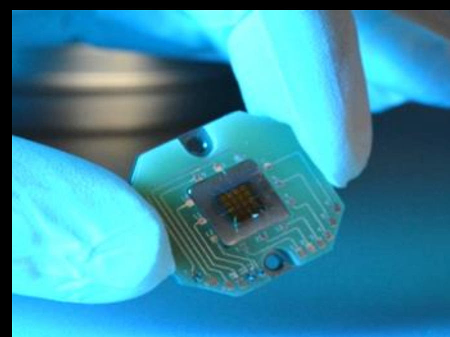
Nadia Belabas @ Goss group http://quantumdot.eu

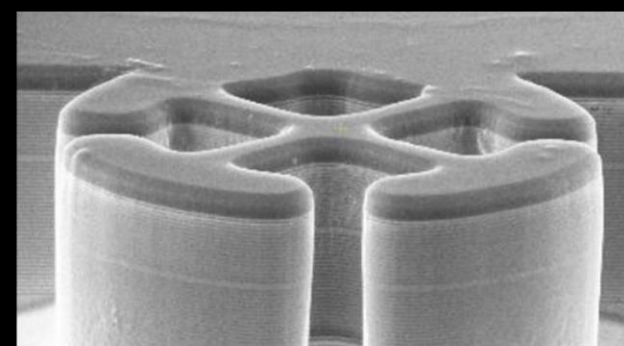
Center for Nanoscience and Nanotechnology C2N
*CNRS – **University** Paris Saclay*

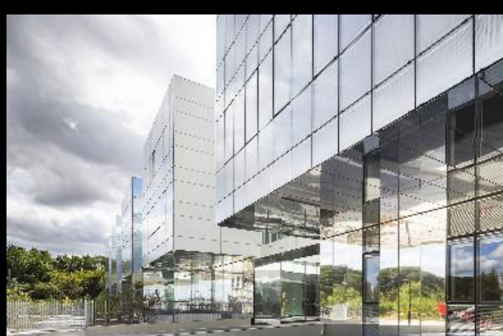


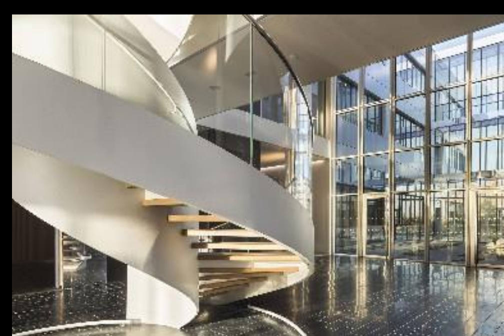
quantum PARIS-SACLAY

Centre de Nanosciences & de Nanotechnologies

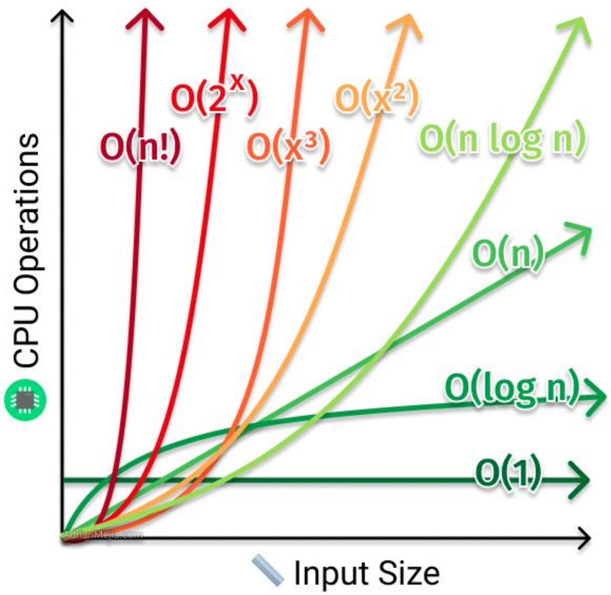


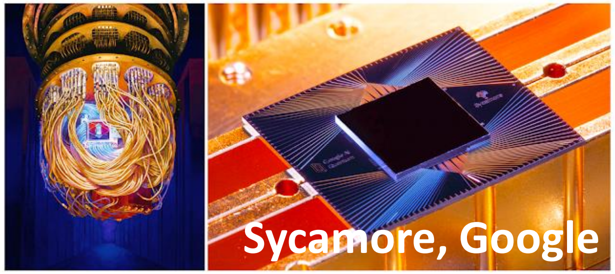






Quantum advantage





Octobre 2019

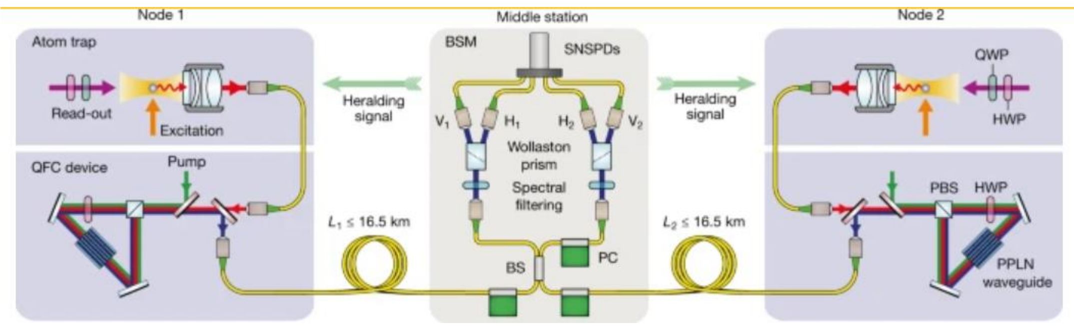
Décembre 2020

Juin 2022

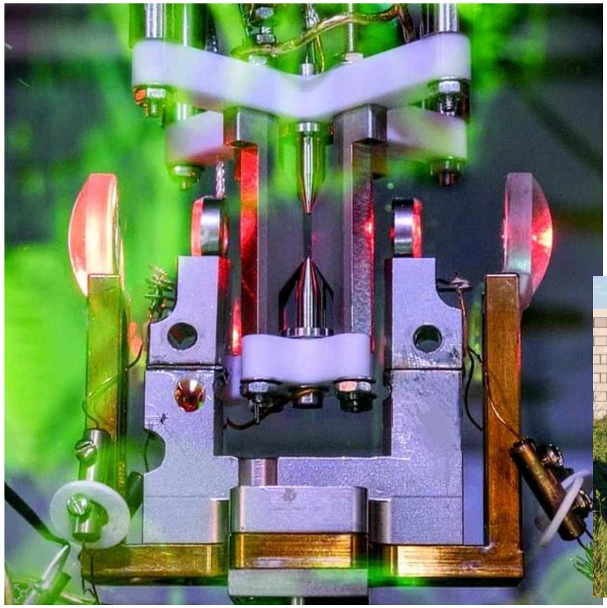
Breaking records for entanglement distances

China's quantum satellite achieves 'spooky action' at record distance

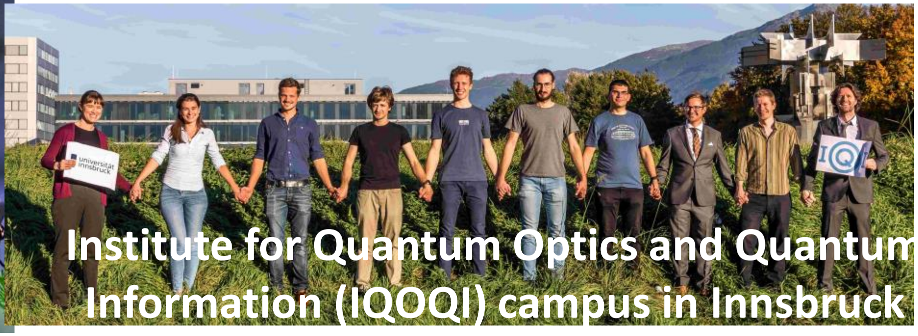
By Gabriel Popkin | Jun. 15, 2017 , 2:00 PM



neutral atoms, juillet 2022, Vienna



Ions, Mai 2023, Innsbruck



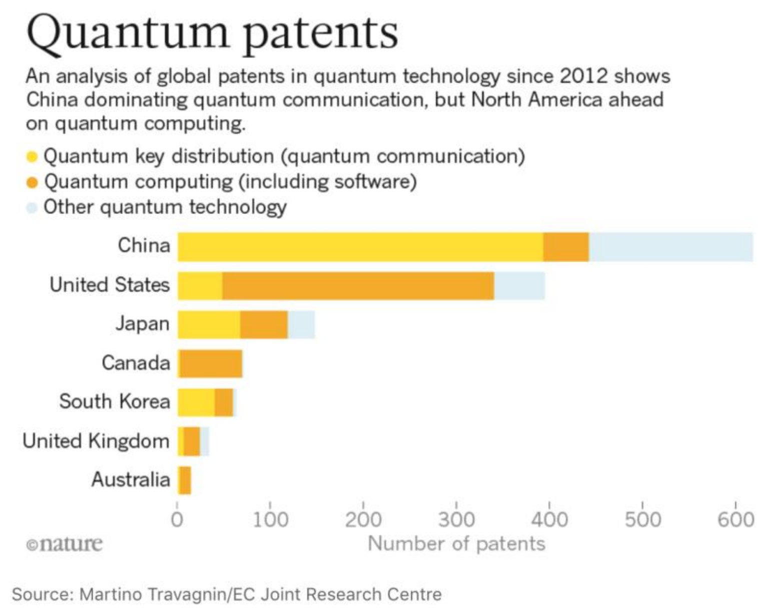
A hot topic for economy

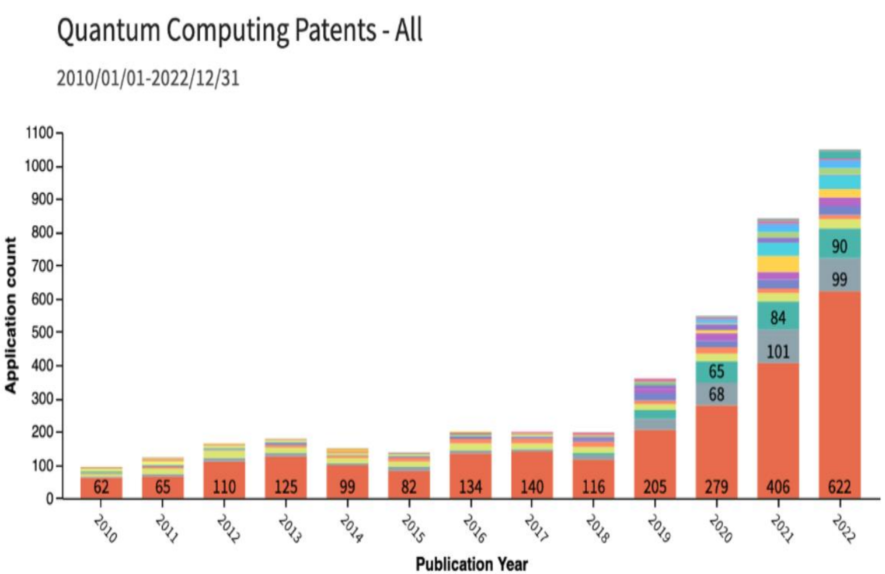
nature Oct 2019 Subscribe

NEWS FEATURE · 02 OCTOBER 2019

Quantum gold rush: the private funding pouring into quantum start-ups

A *Nature* analysis explores the investors betting on quantum technology.





https://quantumconsortium.org/blog/quantum-patent-trends-update-2022/

A hot topic in politics - Sovereignty

The Guardian view on quantum computing: the new space race
Editorial

The main use of quantum technology might not be to hack existing systems but to create unhackable communication networks of the future

Dec 2017

China will open a $10 billion quantum computer center and others also investing in quantum computing

Oct 2017

Brian Wang | October 10, 2017

MIT Technology Review

Dec 2018

Computing Dec 22, 2018

President Trump has signed a $1.2 billion law to boost US quantum tech

Quantum USA Vs. Quantum China: The World's Most Important Technology Race

Moor Insights and Strategy Contributor
Cloud
Straight talk from Moor Insights & Strategy tech industry analysts

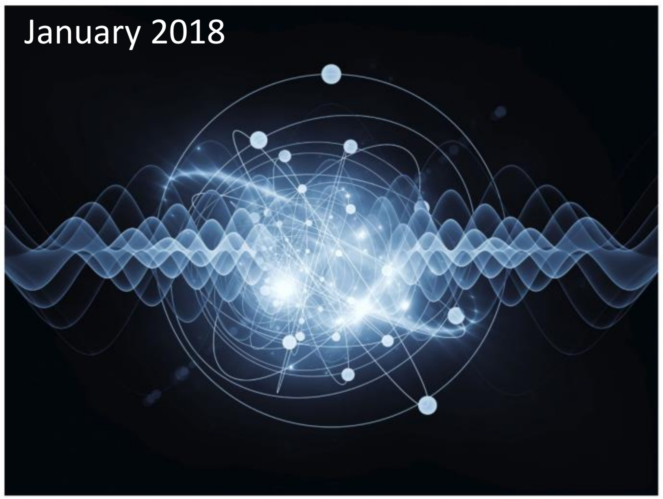
Forbes Oct 2019

European, French initiatives

Quantum Technologies Flagship

The Quantum Technologies Flagship aims to place Europe at the forefront of the second quantum revolution, bringing transformative advances to science, industry and society.

January 2018



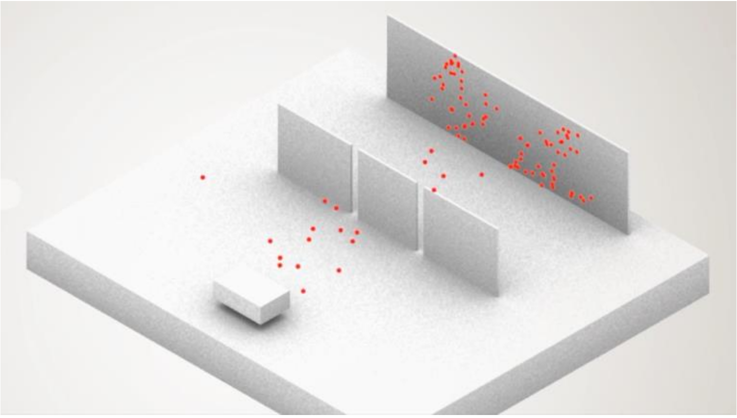
January 2021

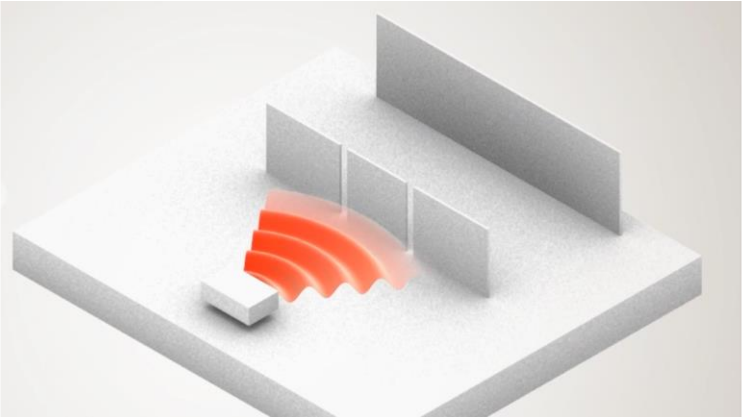
PEPR d'une Stratégie Nationale
Appel à Projets - Calcul Quantique au Vol
2022

PEPR Quantique

Quantum physics and technological revolutions

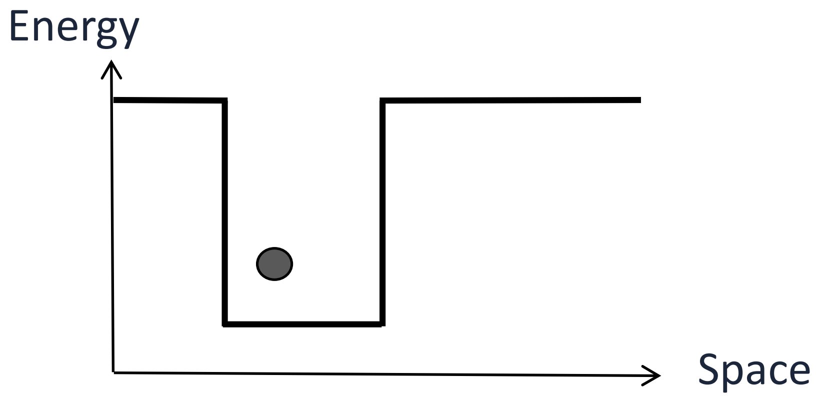
Wave particle duality

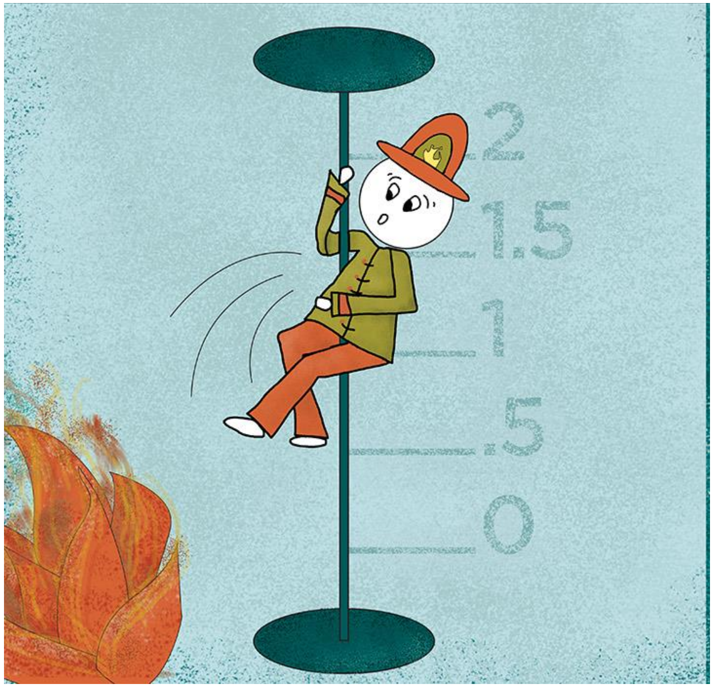




Wave particule duality – J. Bobroff -©vulgarisation.fr

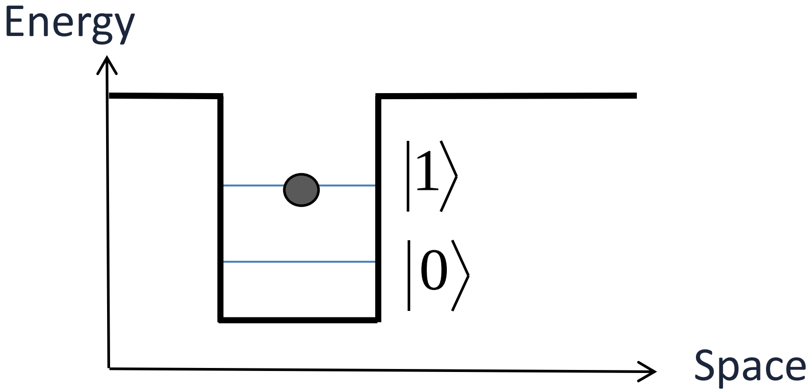
Quantized energy levels





Credit: N. Hanacek/NIST

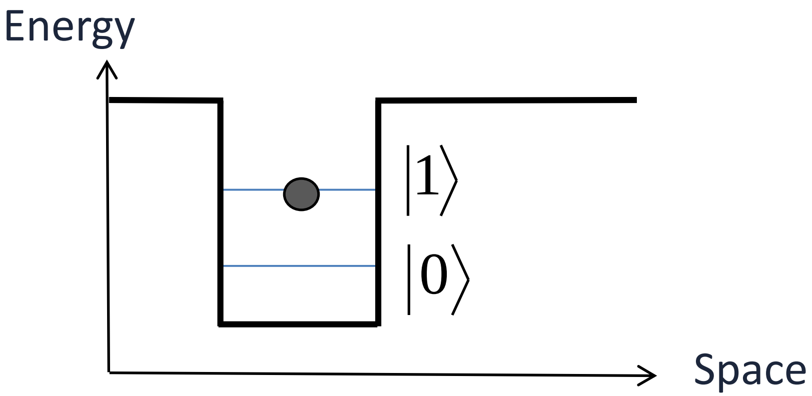
Quantized energy levels

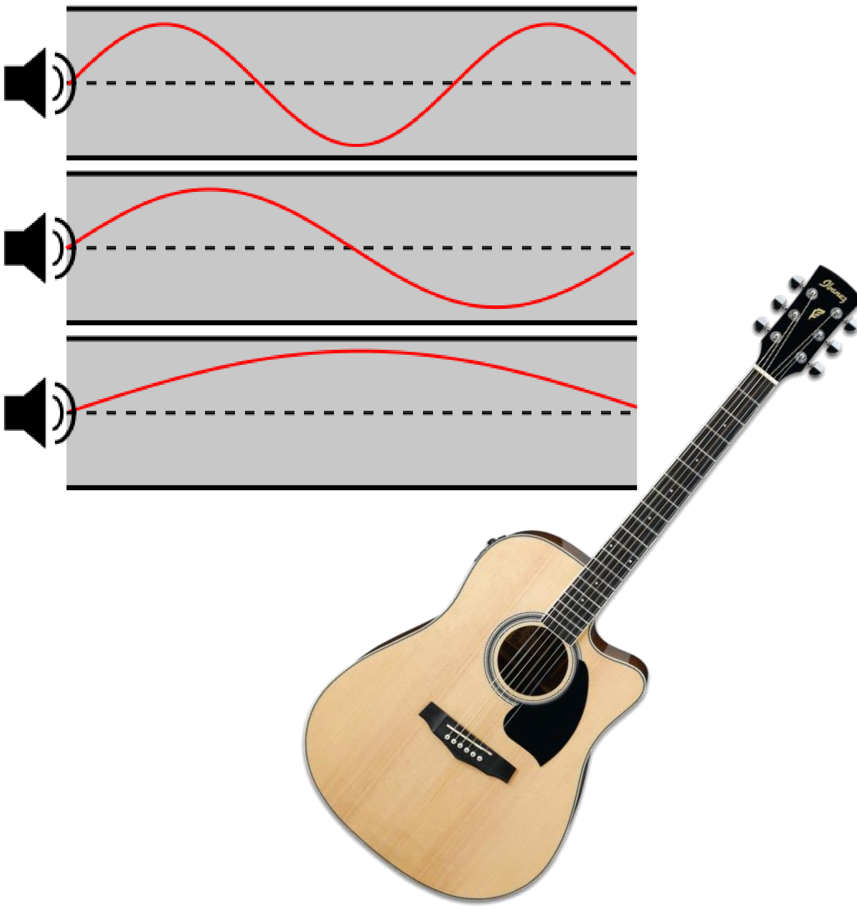


Credit: N. Hanacek/NIST

Basics of quantum revolutions

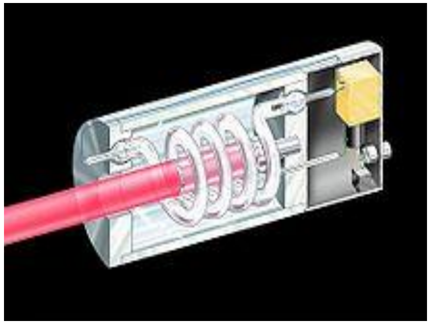
Quantized energy levels



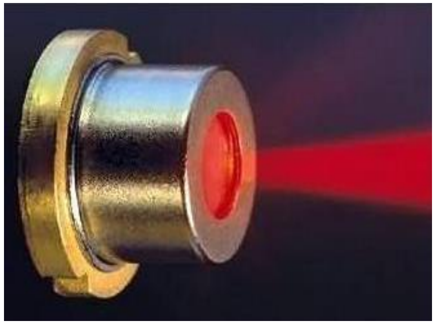


First quantum revolution

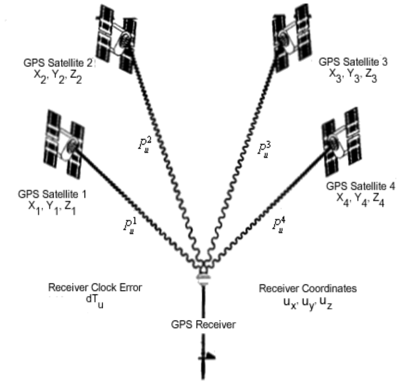
Transistor
1947



Ruby laser
1960



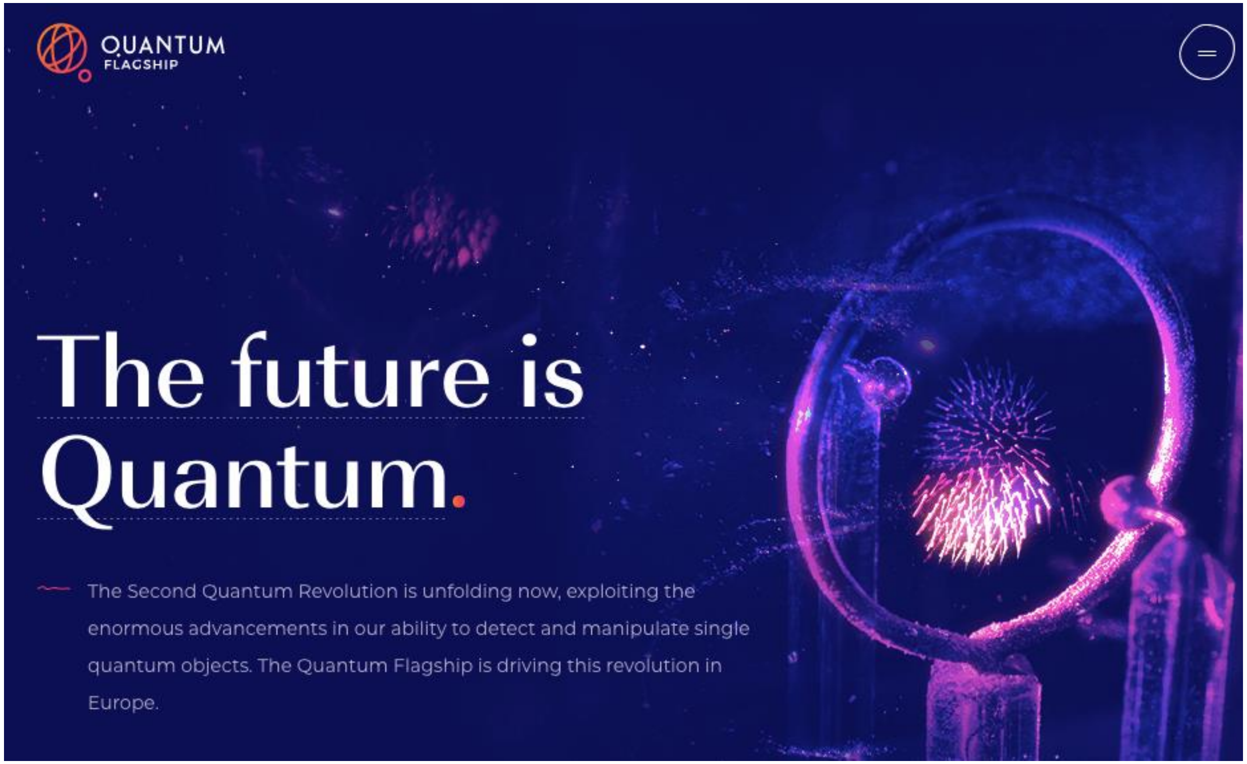
Laser diode
1962



GPS
1995

Precise knowledge and engineering of quantized energy levels

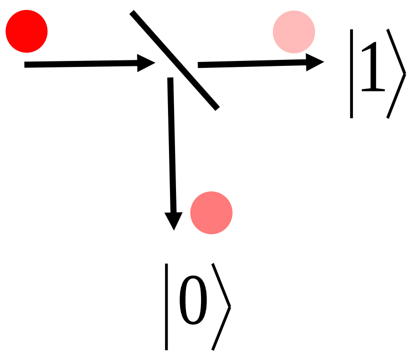
More Quantum to come ?

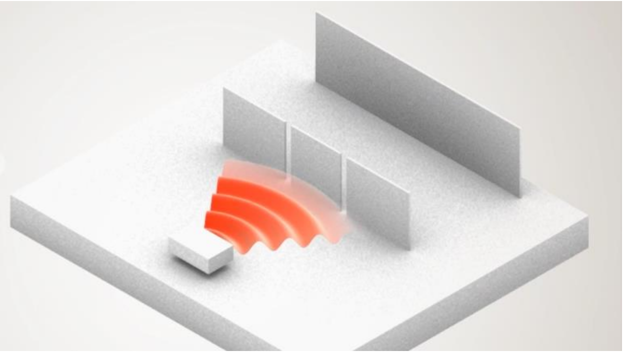


See website for the European Flagship on Quantum Technologies www.qt.eu

-> quantum superposition and entanglement

Coherent superposition

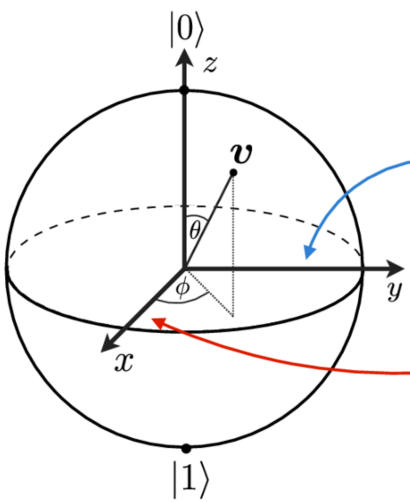




From the classical information bit $|0\rangle$ or $|1\rangle$

… to the quantum bit $a|0\rangle + b|1\rangle$

$$|a|^2 + |b|^2 = 1, \qquad a, b \in \mathbb{C}$$

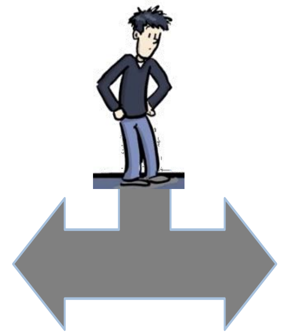


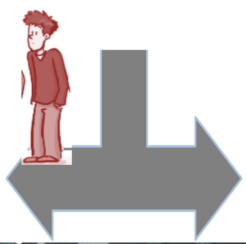
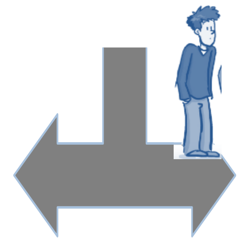
Pole states:

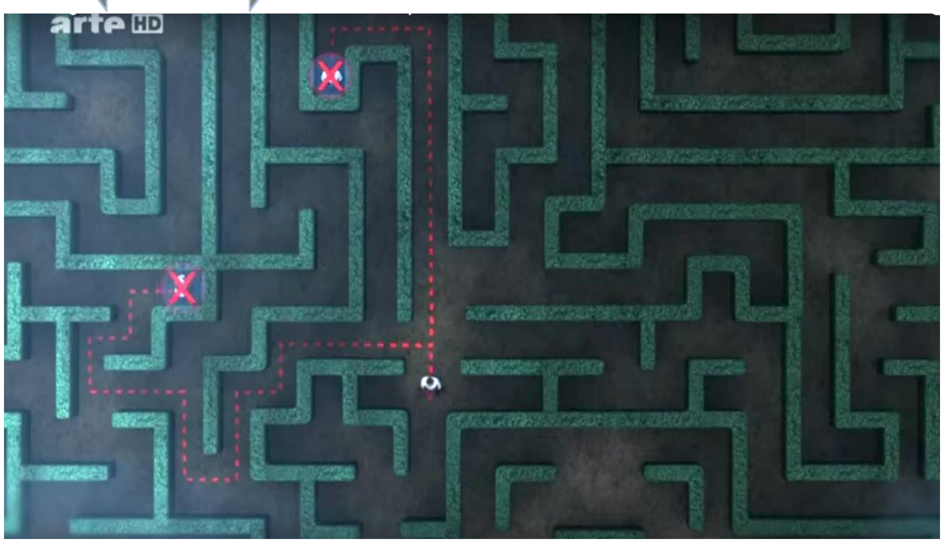
$$|i+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$$
$$|i-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$$

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Finding the way out of a maze



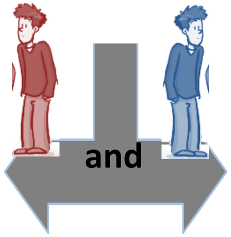
$|0\rangle =$  **or** $|1\rangle =$ 

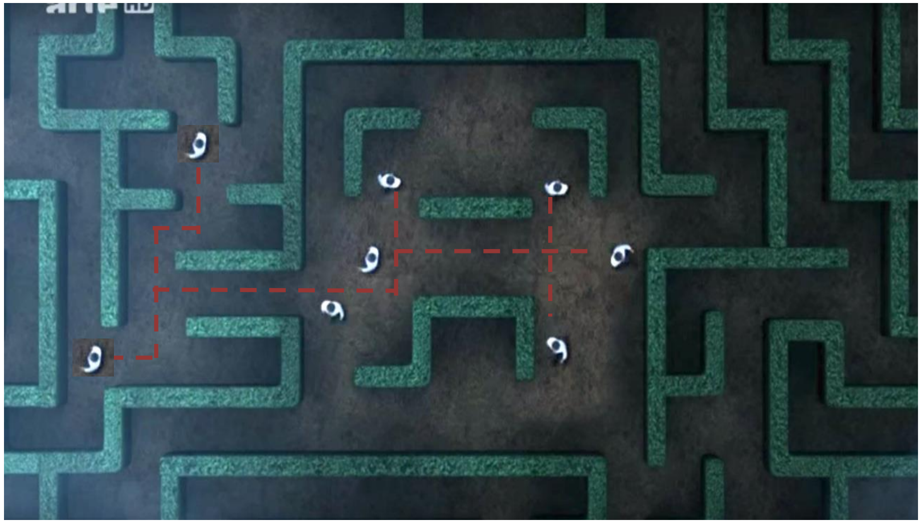


Credit: The Fabric of The Cosmos: Quantum Leap

Gain for Quantum computer ?

$$|y\rangle = a|0\rangle + b|1\rangle$$

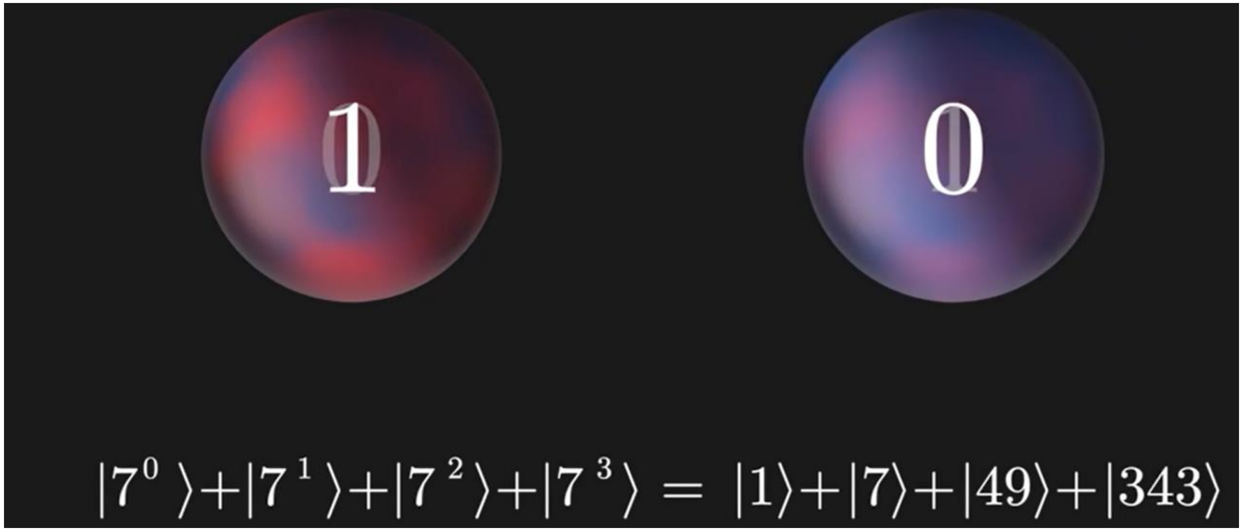


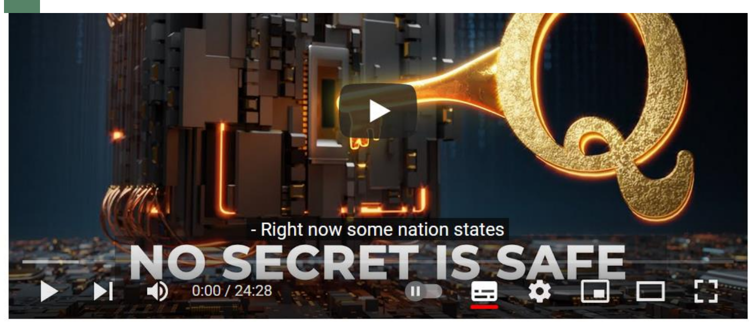


Credit: The Fabric of The Cosmos: Quantum Leap

Superposition is powerful
but the « parallel » image is misleading

Calculating 7^n as a step of Shor algorithm



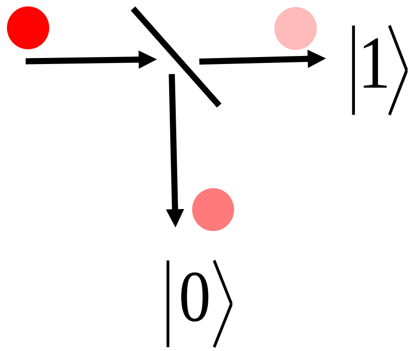


How Quantum Computers Break The Internet... Starting Now

Veritasium
an element of truth

Credit: Veritasium – How computers break the internet …starting now

Measurement



Quantum bit $a|0\rangle + b|1\rangle$ with $|a|^2 + |b|^2 = 1$

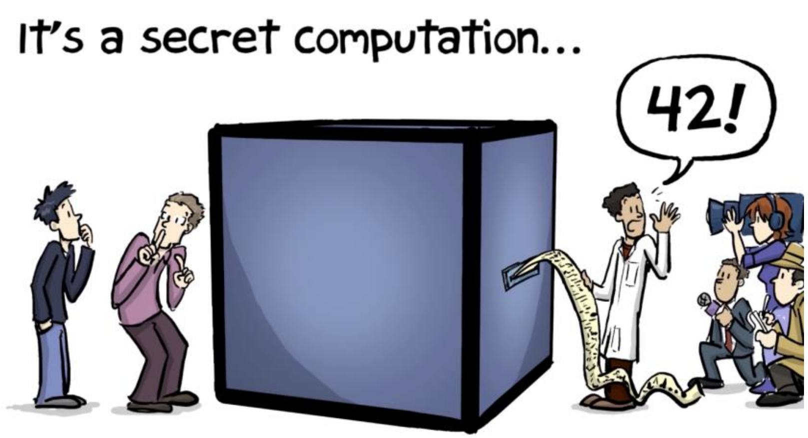
Measurement:

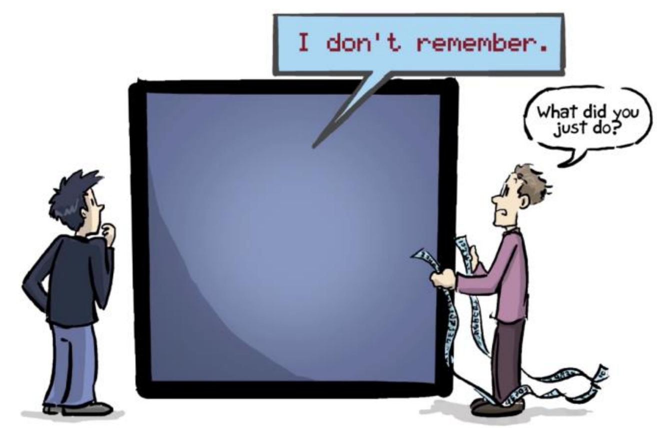
- Probability $|a|^2$ to measure the qubit in the state $|0\rangle$

  $\Rightarrow$ After measurement qubit state = $|0\rangle$

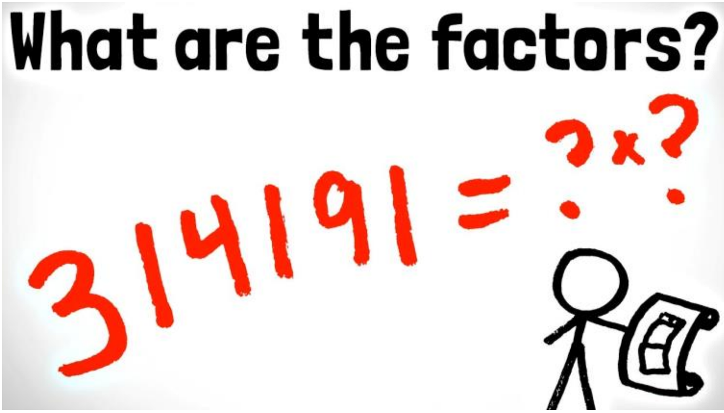
- Probability $|b|^2$ to measure the qubit in the state $|1\rangle$

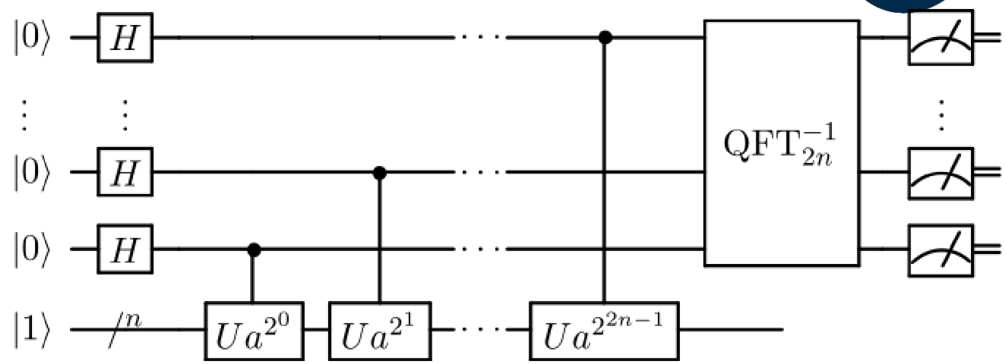
  => After measurement qubit state = $|1\rangle$





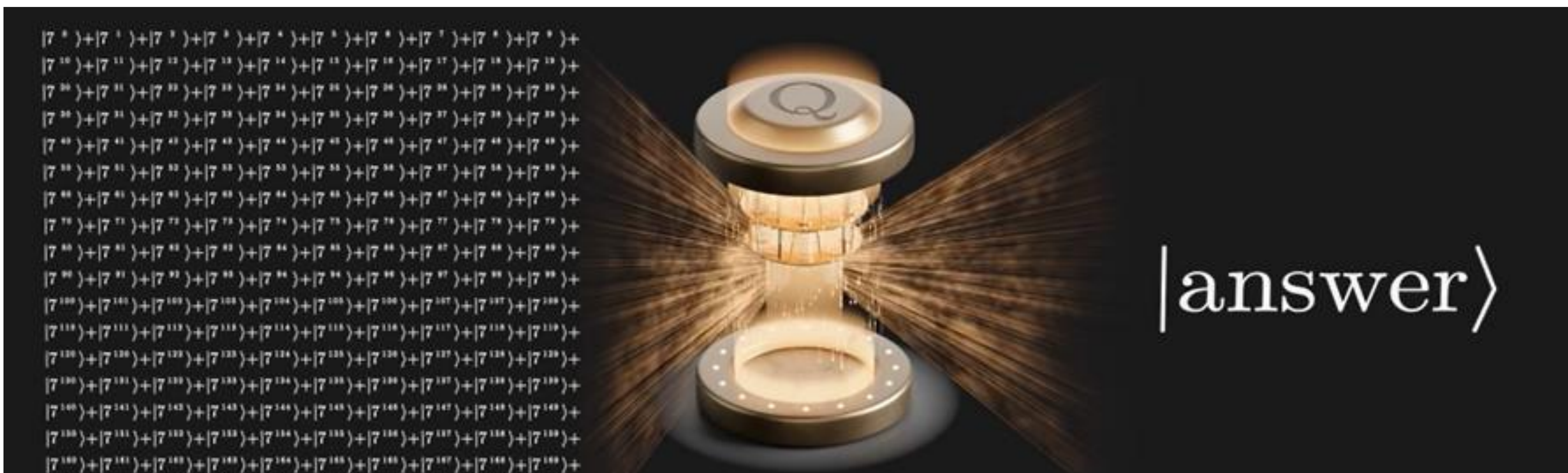
Quantum computer magical power ?





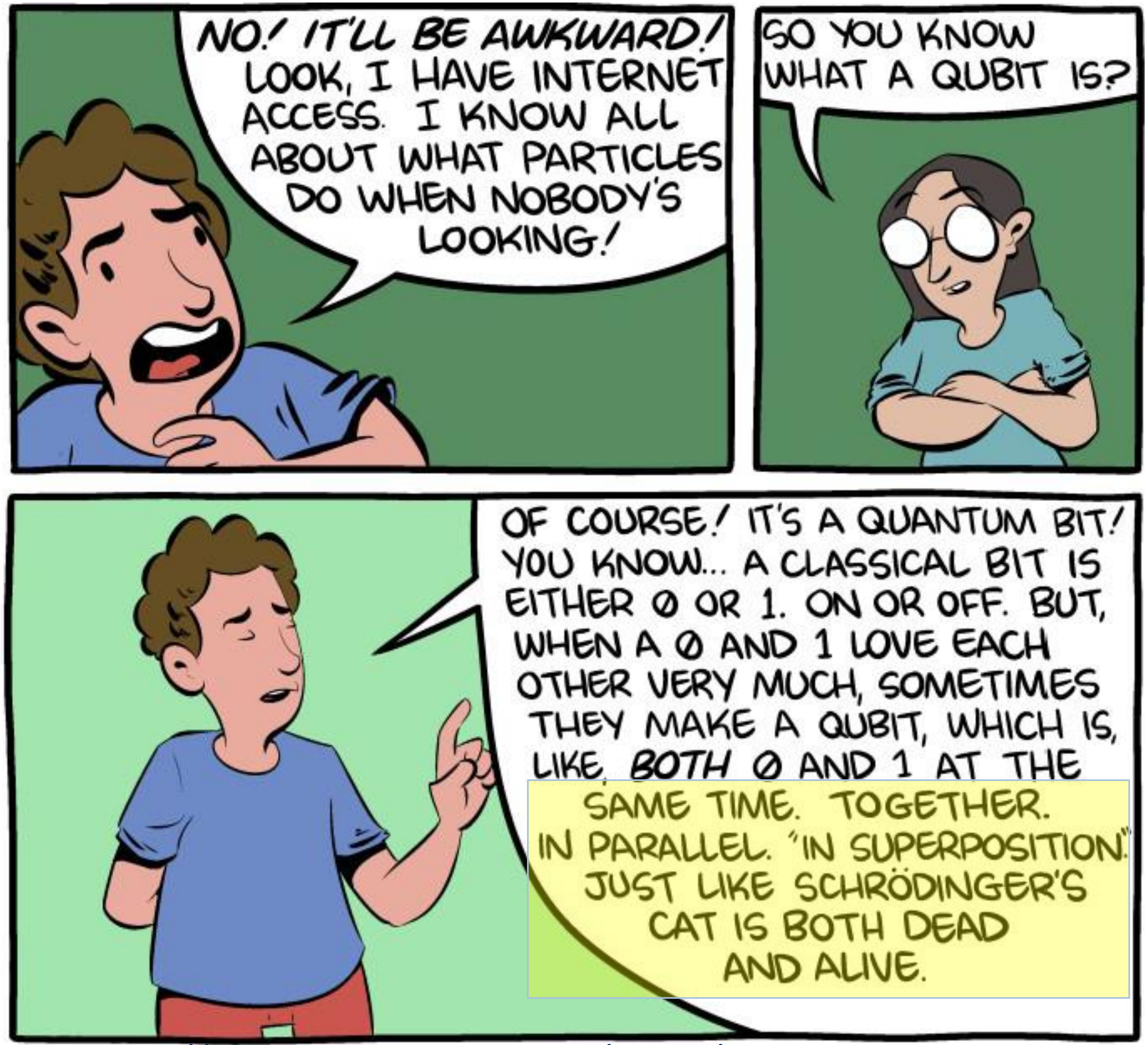
Shor - Quantum subroutine

Calculating 7^n as a step of Shor algorithm



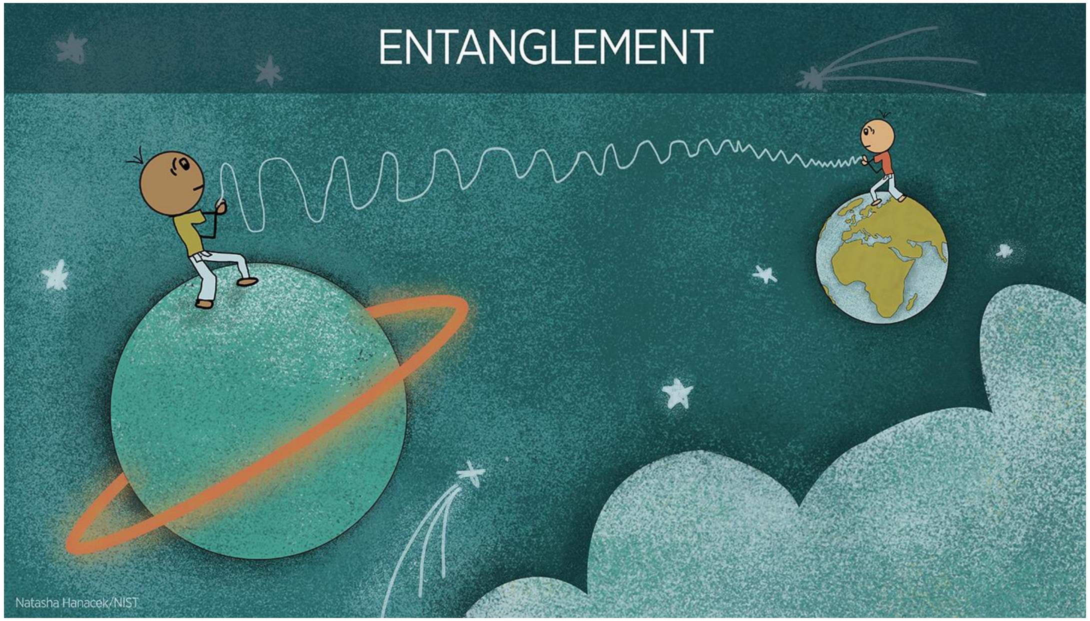
Credit: Veritasium – How computers break the internet …starting now

https://www.smbc-comics.com/comic/the-talk-3



https://www.smbc-comics.com/comic/the-talk-3

2nd ingredient: entanglement



Credit: N. Hanacek/NIST

2nd ingredient: entanglement

Entangled state for two particules A and B

$$\frac{|0_A, 0_B\rangle + |1_A, 1_B\rangle}{\sqrt{2}}$$

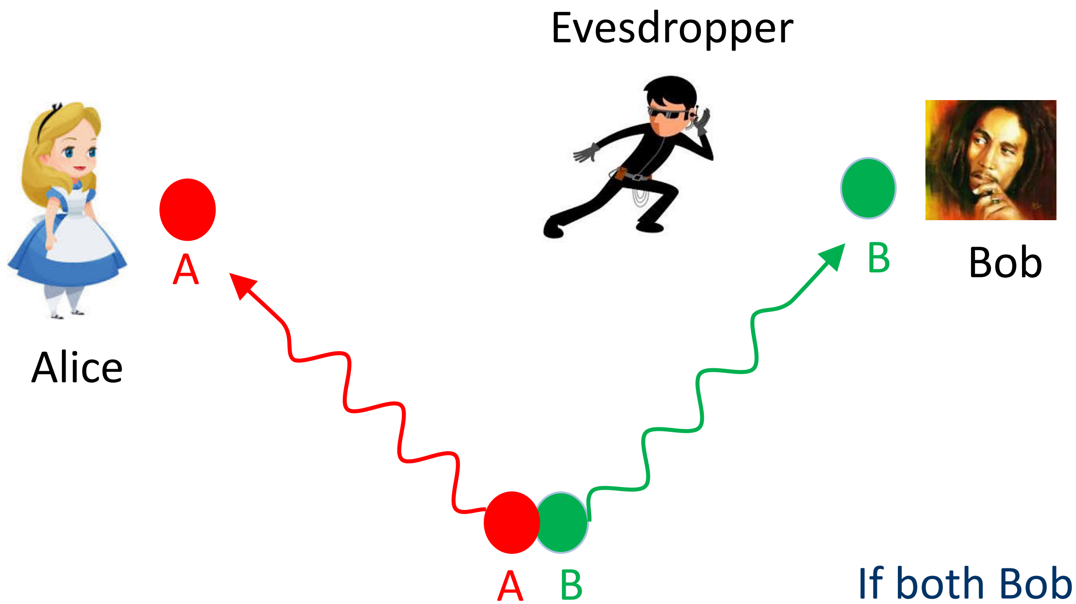
If A is measured in state 0, then B is in state 0

If A is measured in state 1, then B is in state 1

Two particles with a common fate

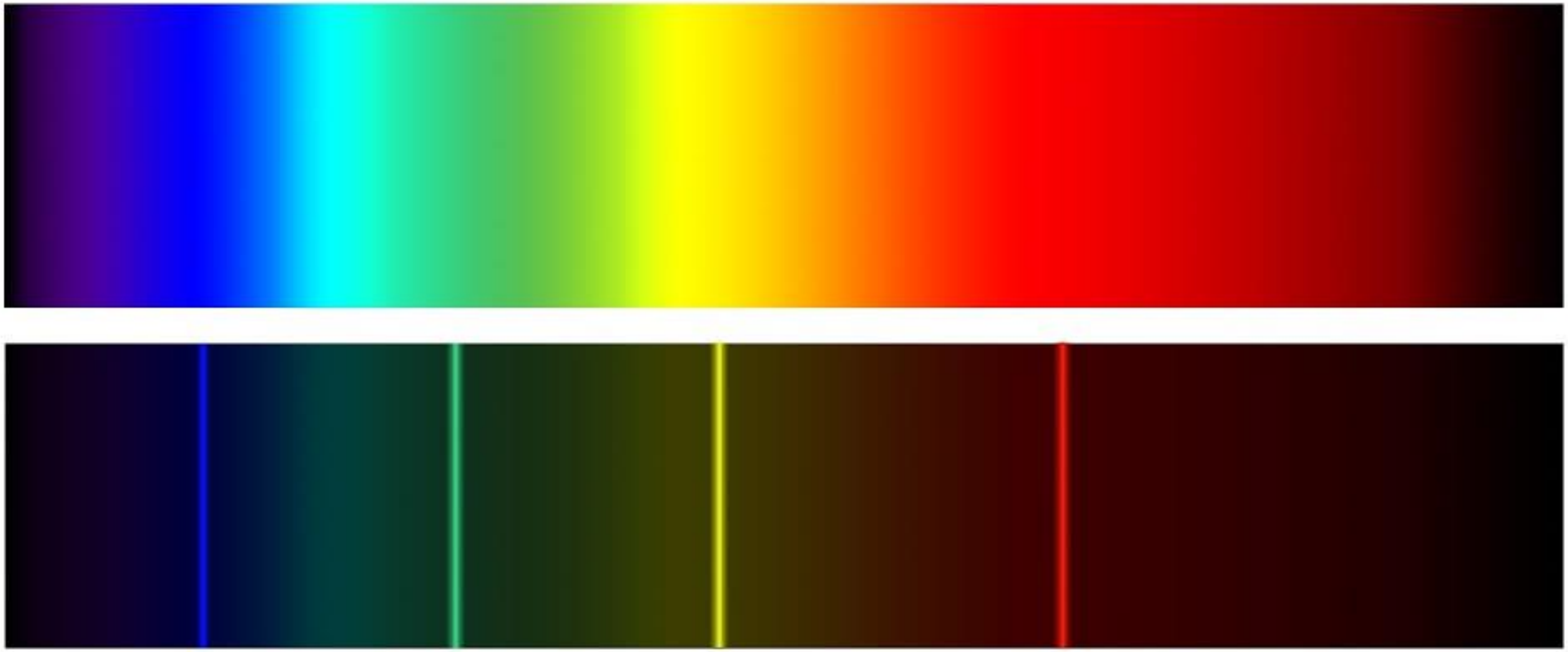
Entanglement for secure quantum communications

or



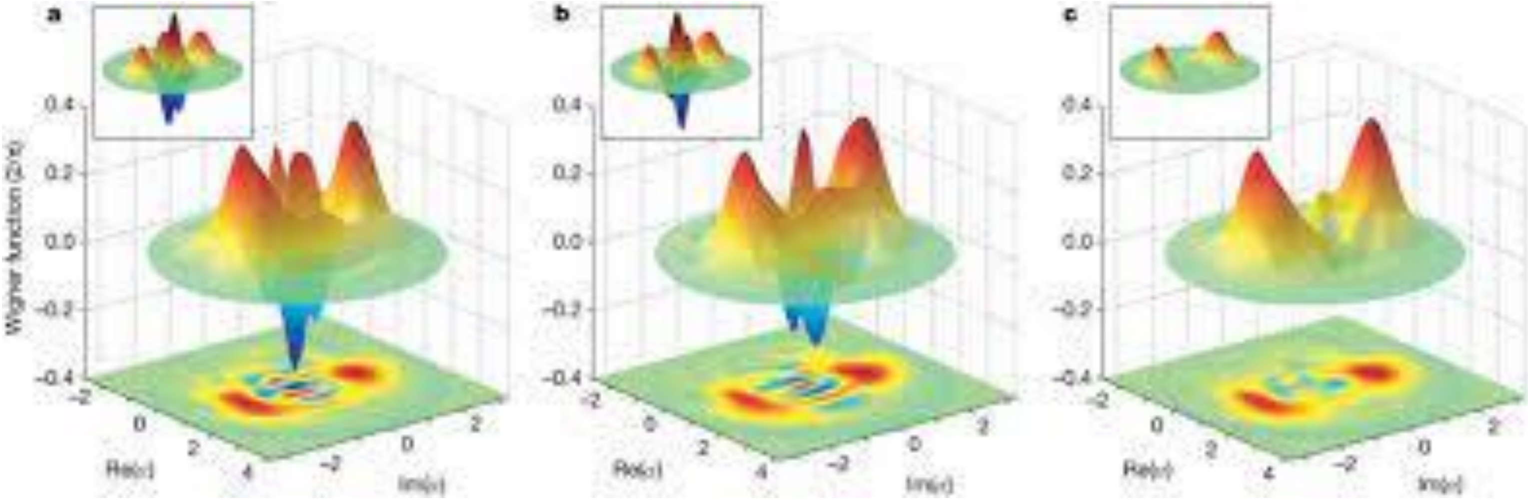
If both Bob and Alice measure a photon, they share the same information

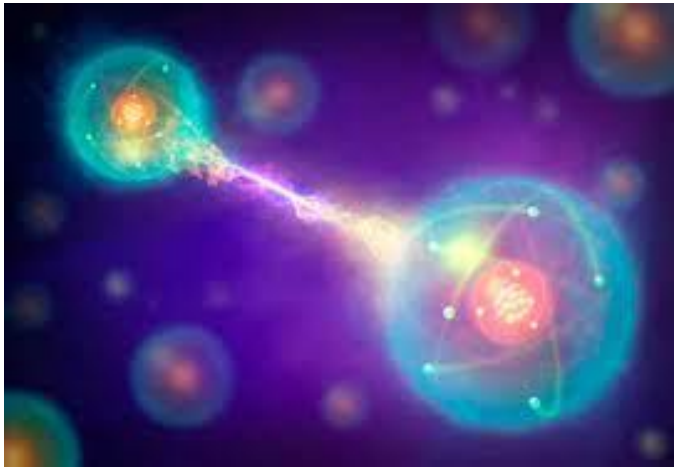
Summary : First quantum revolution



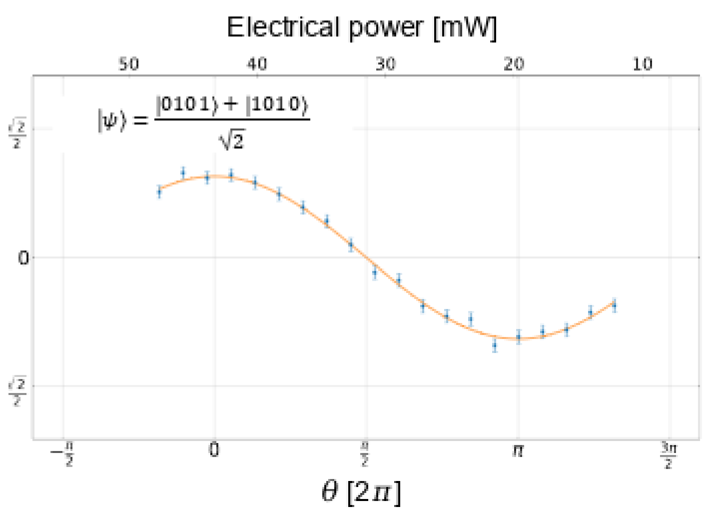
 

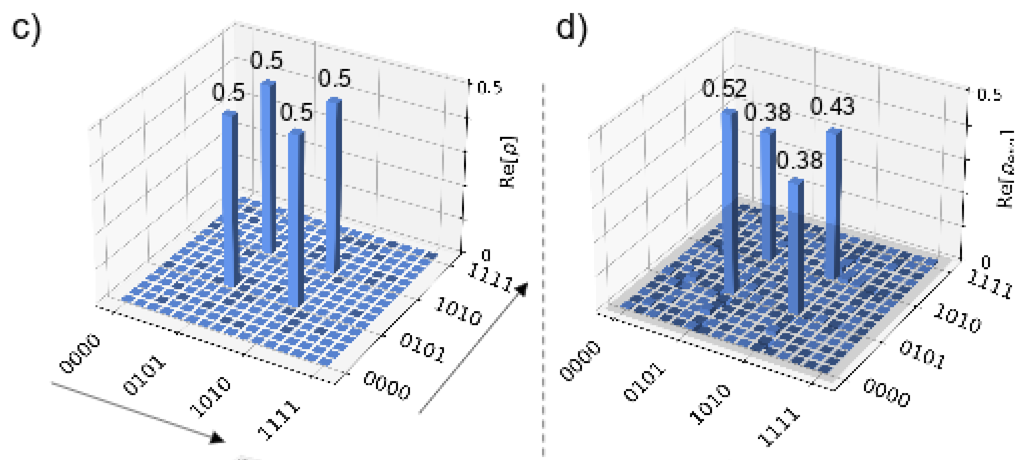
Superposition



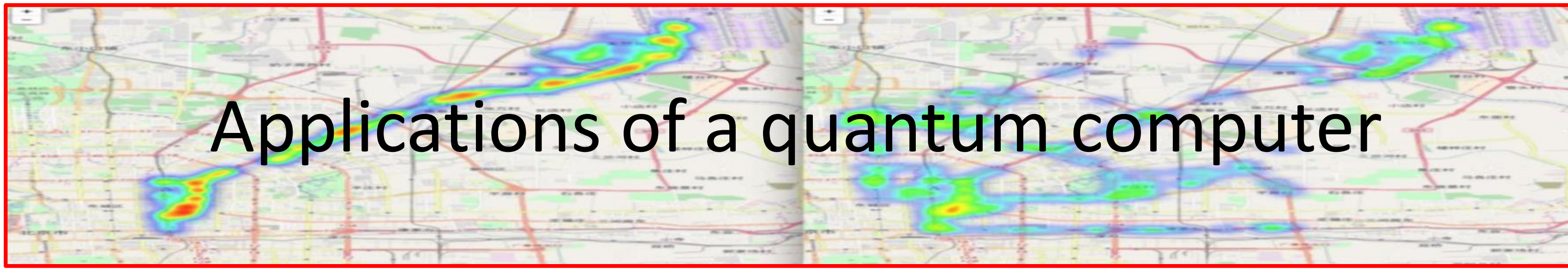


Entanglement – Quantum correlations Vs Classical correlations

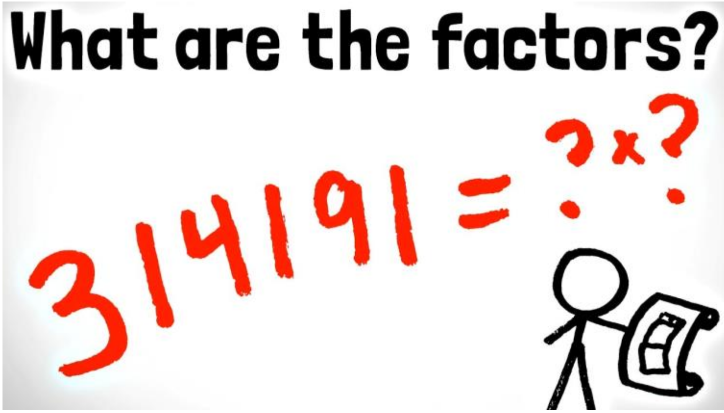




Applications of a quantum computer

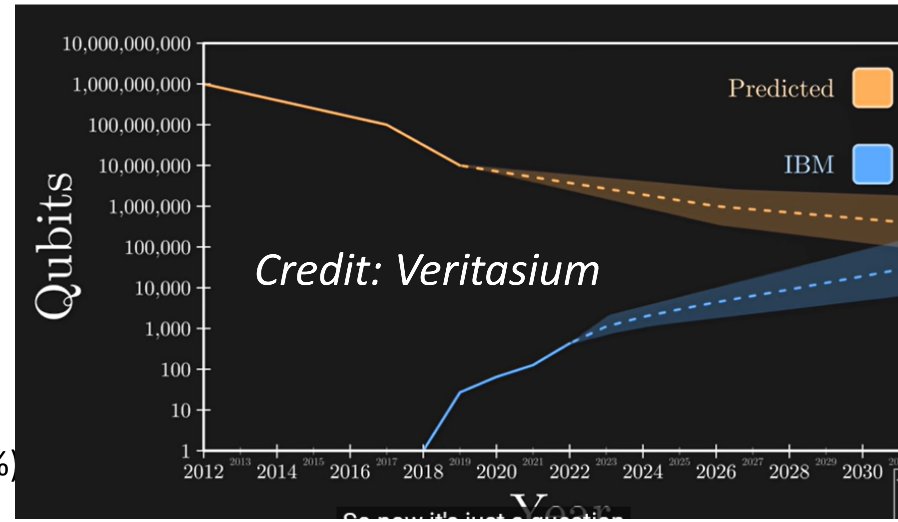


Decipher cryptography



Public-key cryptography:

hardness of factorizing prime numbers



Requires tens of millions of excellent quantum bits and gates

(error <0.1%)

SIAM J. COMPUT.
Vol. 26, No. 5, pp. 1484–1509, October 1997

POLYNOMIAL-TIME ALGORITHMS FOR PRIME FACTORIZATION AND DISCRETE LOGARITHMS ON A QUANTUM COMPUTER*

PETER W. SHOR†

Abstract. A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

Shor algorithm threat

Computational response: Post-quantum cryptography

Principe: Develop cryptography protocols that resist quantum computational power

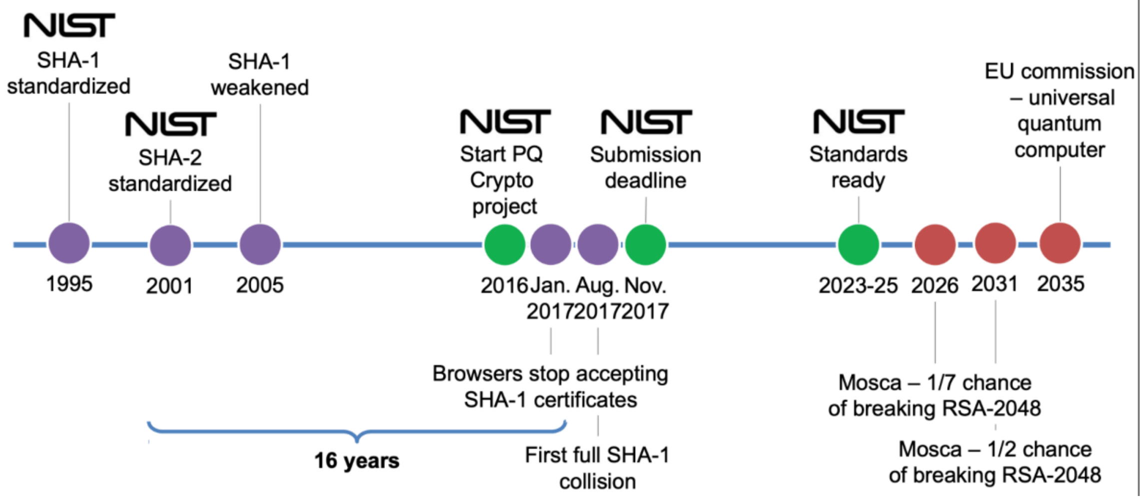
NIST Announces First Four Quantum-Resistant Cryptographic Algorithms

Federal agency reveals the first group of winners from its six-year competition.

July 05, 2022

https://www.linkedin.com/feed/update/urn:li:activity:7087508273540517888/

NIST time line to define new encryption standards



Credit: Douglas Stebila - Waterloo

Post-quantum crypto

Classical crypto with no known exponential quantum speedup

Hash- & symmetric-based
- Merkle signatures
- Sphincs
- Picnic

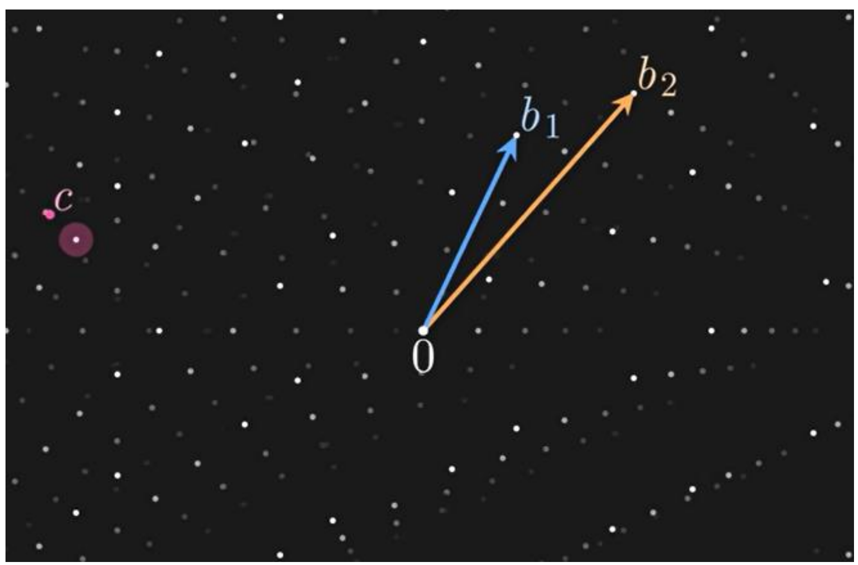
Code-based
- McEliece
- Niederreiter

Multivariate
- multivariate quadratic

Lattice-based
- NTRU
- learning with errors
- ring-LWE, …
- LWrounding

Isogenies
- supersingular elliptic curve isogenies

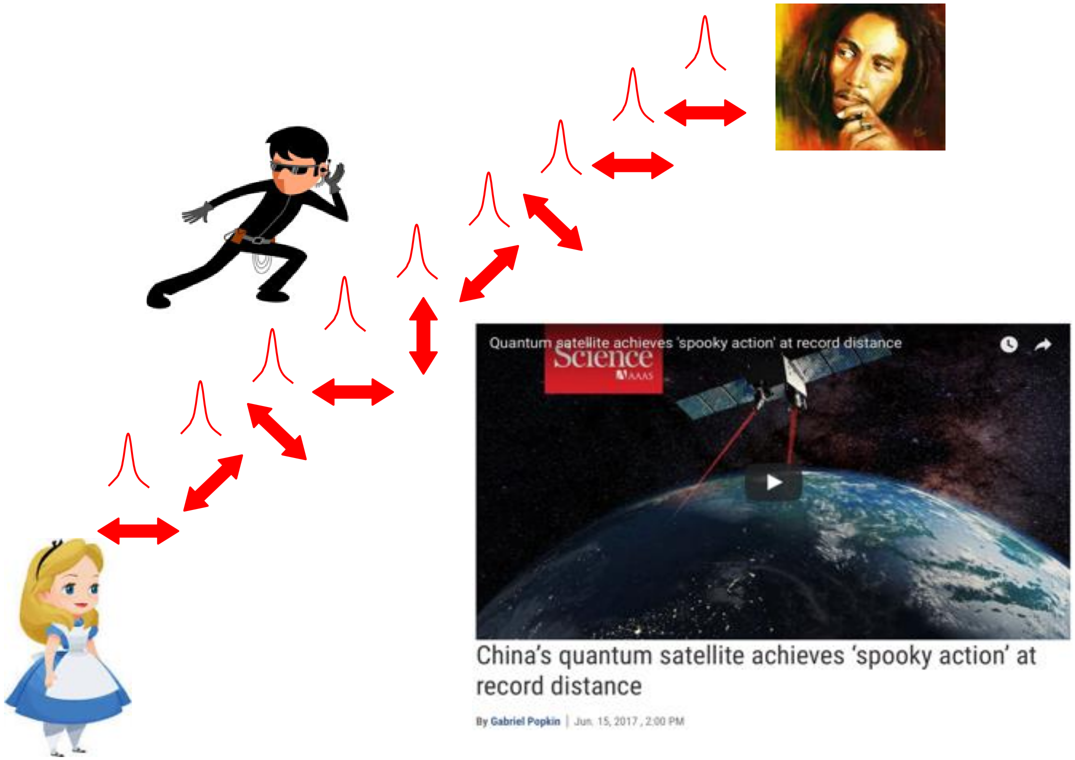
Credit: Douglas Stebila - Waterloo



Credit: Veritasium
– How computers break the internet …starting now

Shor algorithm threat

Hardware response: Quantum cryptography



China's quantum satellite achieves 'spooky action' at record distance

By Gabriel Popkin | Jun. 15, 2017 , 2:00 PM

China quantum cryptography infrastructures

Credit: Erik Vrielink

BB84: first quantum cryptography protocol
Developed by C.Bennett and G.Brassard in 1984

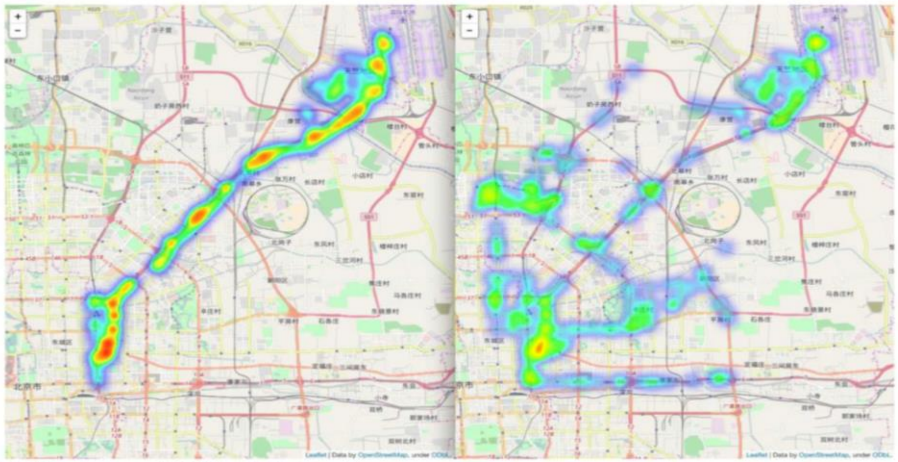
Applications of a universal quantum computer

Where High Power Computation (HPC) is needed:

- Machine learning, Big data
- Optimisation problems (traffic, energy)
- Quantum and physics simulations (new materials, new molecules)
- Cybersecurity
- Finances…

..an ever growing list as industrials get involved

Dwave quantum annealing computer (since 2010) on Traffic flow (2017)



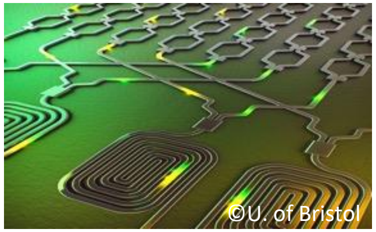
arXiv:1708.01625 Quadratic Unconstraint Binary Optimisation

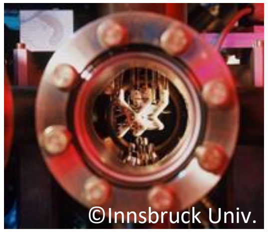

1935

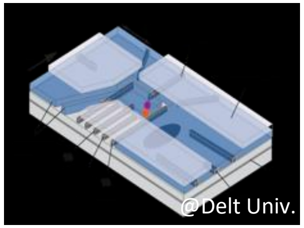

THINK
Late 1940’s

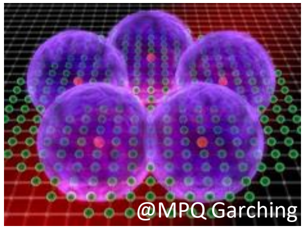
?

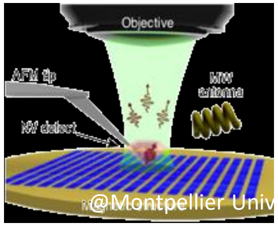
Many kinds and flavors of qubits





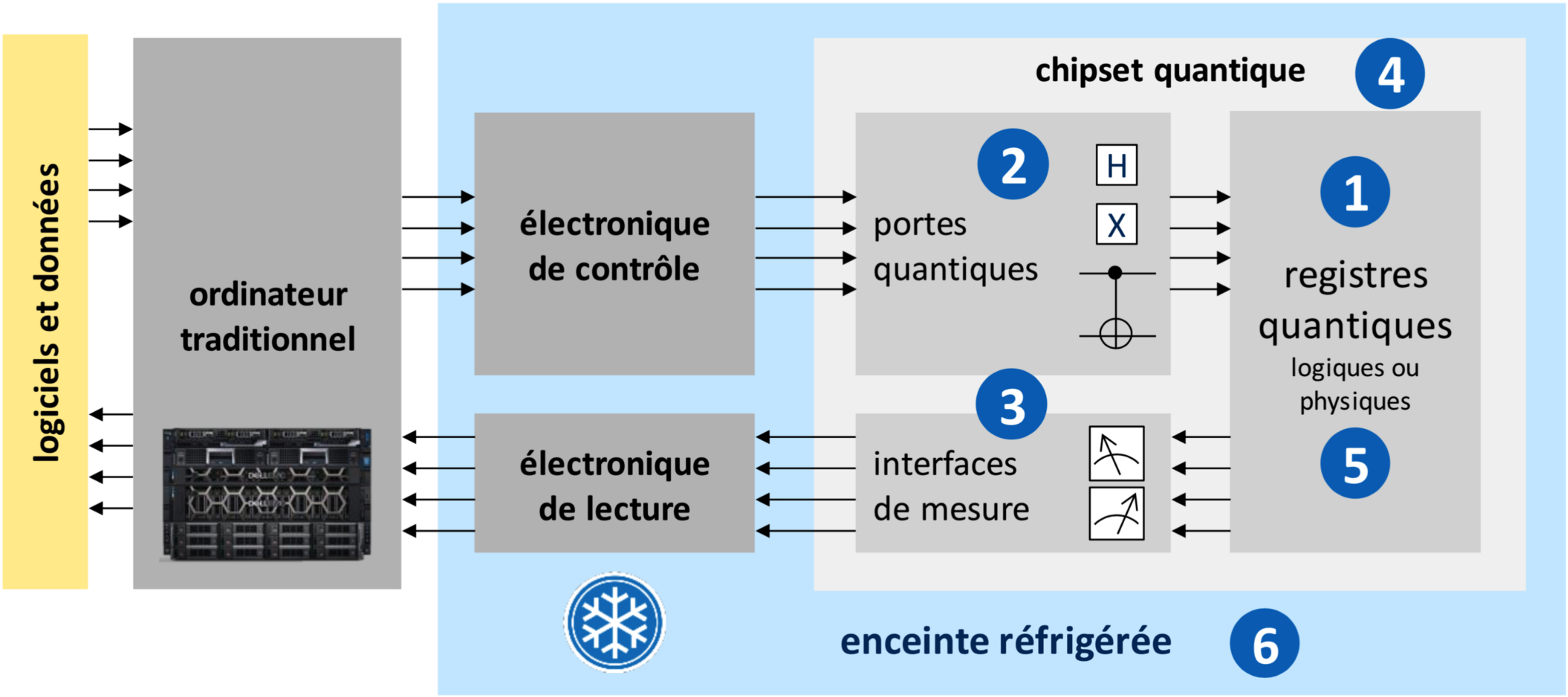






Basics of a quantum computer

Quantum computer architecture
Co-processor



Quantum computer ingredients

DiVincenzo's criteria

2000 @ IBM

Article Talk

From Wikipedia, the free encyclopedia

The **DiVincenzo criteria** are conditions necessary for constructing a quantum c
physicist David P. DiVincenzo,[1] as being those necessary to construct such a c
Manin, in 1980,[2] and physicist Richard Feynman, in 1982[3]—as a means to ef
quantum many-body problem.

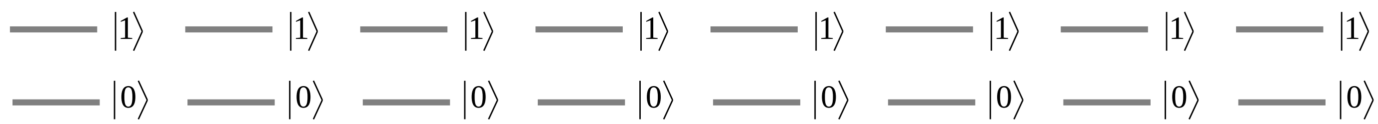
- A scalable physical system with well characterized qubits
- The ability to initialize the state of the qubits
- A qubit-specific measurement capability
- A "universal" set of quantum gates
- Long decoherence times

DiVincenzo, David P. (2000-04-13). "The Physical Implementation of Quantum Computation". Fortschritte der Physik. 48 (9–11): 771–783.

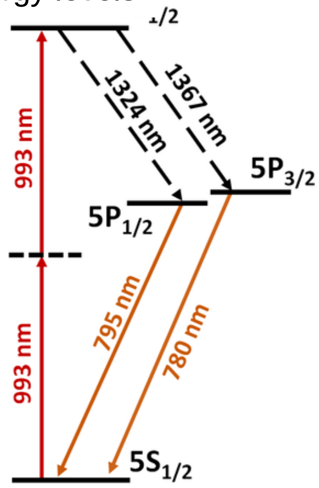
Quantum computer ingredients

(Di Vicenzo's criteria)

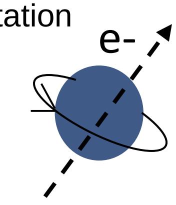
- A scalable physical system with well characterized qubits

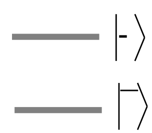


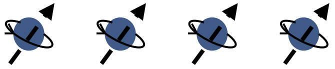
Atom energy levels



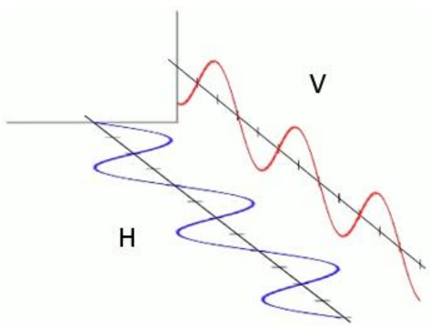
Spin orientation







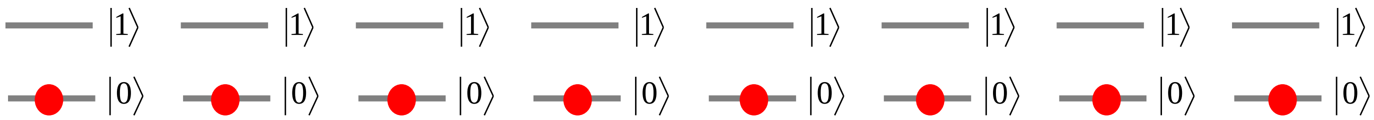
Photon polarization

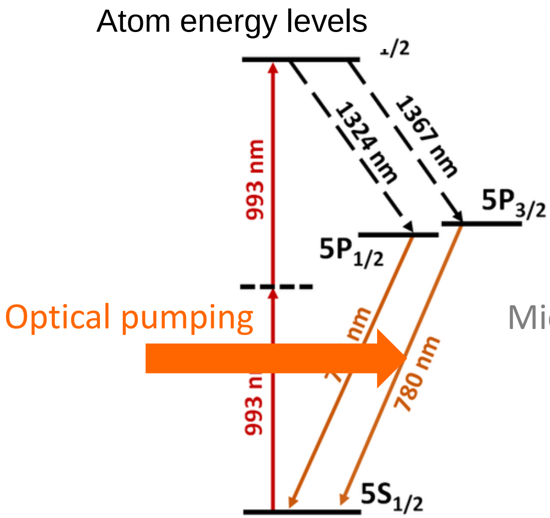


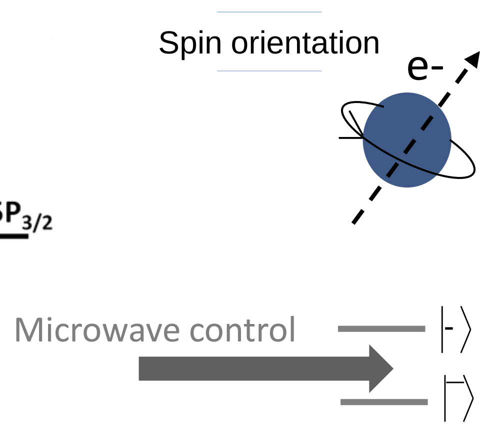
Quantum computer ingredients

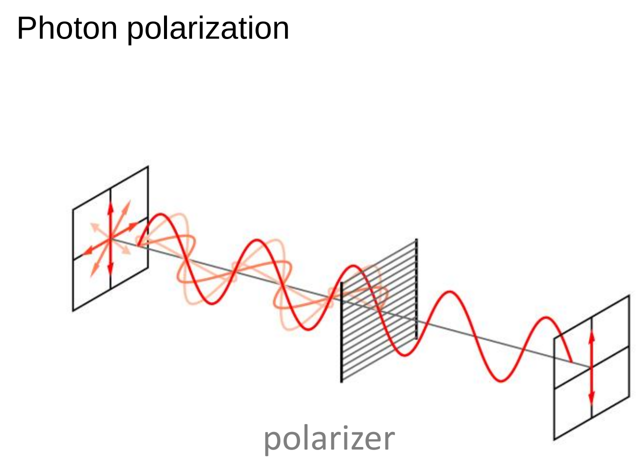
(Di Vicenzo's criteria)

- The ability to initialize the state of the qubits





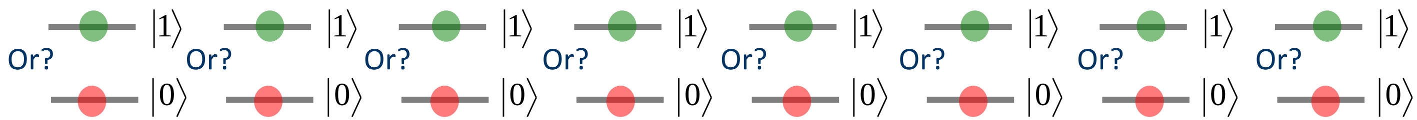




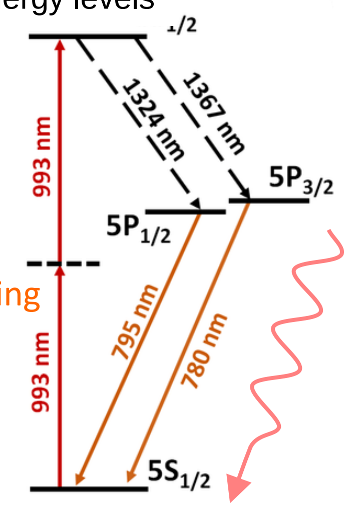
Quantum computer ingredients

(Di Vicenzo's criteria)

- A qubit-specific measurement capability



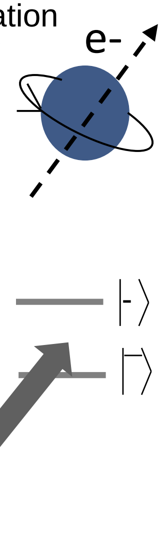
Atom energy levels



Optical pumping

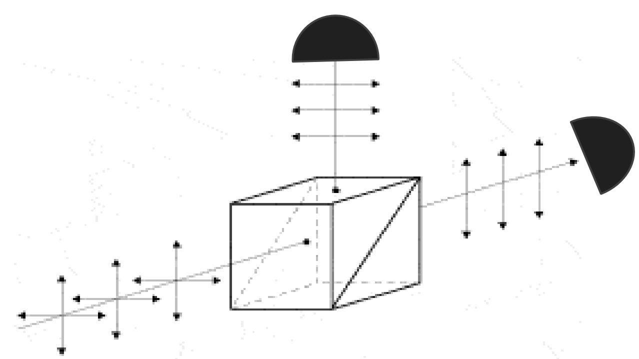
Fluorescence

Spin orientation



Microwave readout

Photon polarization



Polarizer + single photon detectors

Quantum computer ingredients

(Di Vicenzo's criteria)

- A "universal" set of quantum gates :

- Single qubit gates

$\longrightarrow a|0\rangle + b|1\rangle$

Pauli-X (X)	X	$\oplus$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)	Y		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)	Z		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)	H		$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

$$a|0\rangle + b|1\rangle \longrightarrow b|0\rangle + a|1\rangle$$

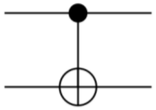
$$|0\rangle \longrightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

DiVincenzo, David P. (2000-04-13). "The Physical Implementation of Quantum Computation". Fortschritte der Physik. 48 (9–11): 771–783.

- A "universal" set of quantum gates :

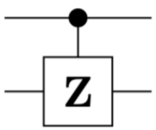
- Two qubit gates

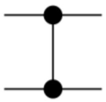
Controlled Not (CNOT, CX)



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

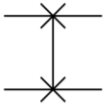
Controlled Z (CZ)





$$\begin{bmatrix}1 & 0 & 0 & 0\\0 & 1 & 0 & 0\\0 & 0 & 1 & 0\\0 & 0 & 0 & -1\end{bmatrix}$$

SWAP

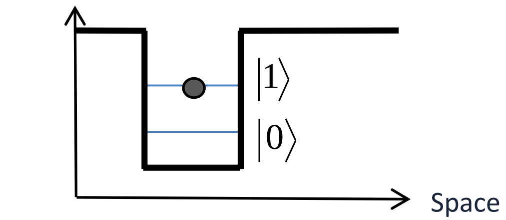


$$\begin{bmatrix}1 & 0 & 0 & 0\\0 & 0 & 1 & 0\\0 & 1 & 0 & 0\\0 & 0 & 0 & 1\end{bmatrix}$$

DiVincenzo, David P. (2000-04-13). "The Physical Implementation of Quantum Computation". Fortschritte der Physik. 48 (9–11): 771–783.

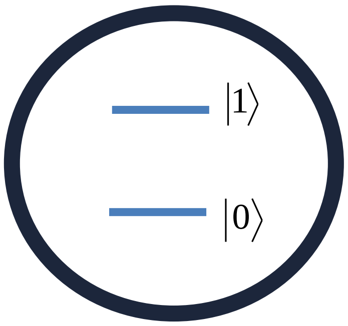
The enemy : decoherence

- Long decoherence times



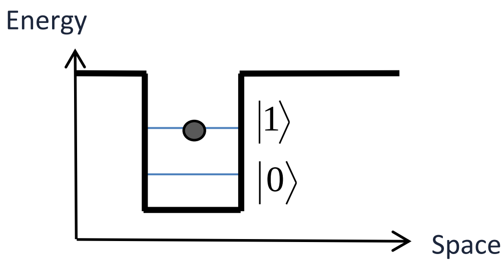
quantum bit $a|0\rangle + b|1\rangle$ with $|a|^2 + |b|^2 = 1$

Isolated quantum bit



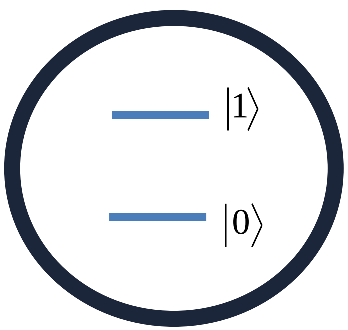
The enemy : decoherence

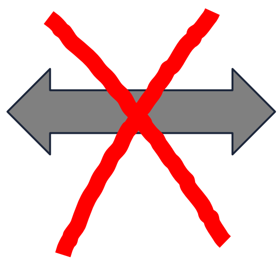
- Long decoherence times



quantum bit $a|0\rangle + b|1\rangle$ with $|a|^2 + |b|^2 = 1$

Isolated quantum bit



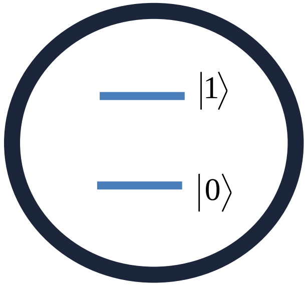


Large reservoir of states:

Mechanical vibration
Fluctuating charges
Fluctuating spins
…

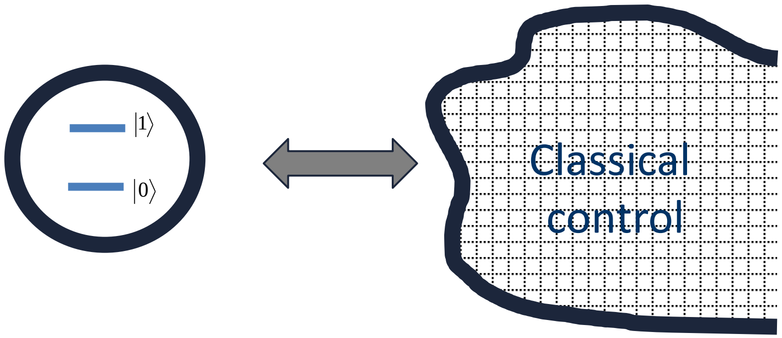
Irreversible loss of energy and/or information

Necessary compromises

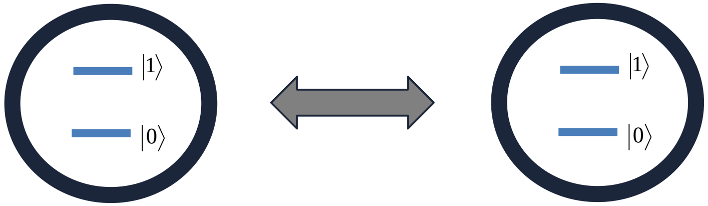


No decoherence ➡ Isolated quantum bit

But coupling to the outside world necessary

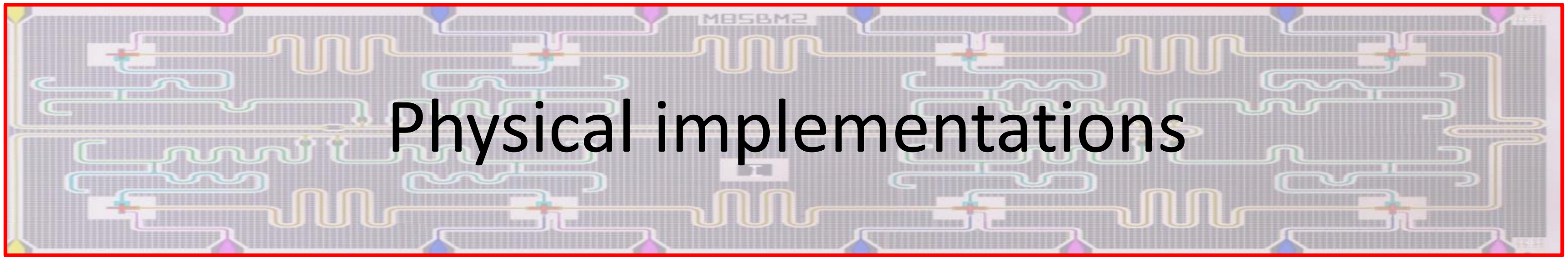


To manipulate the quantum bit



To implement 2 quantum bit gates

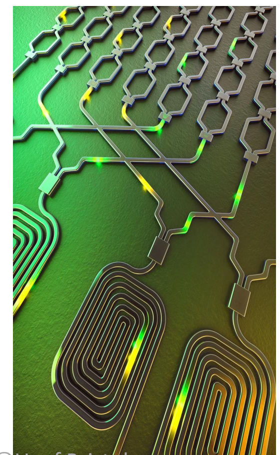
Physical implementations



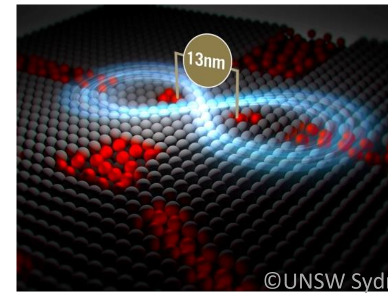
Leading platforms

Superconducting
qubits

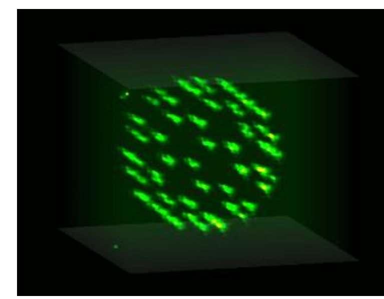
Trapped ions



Photons



Silicon qubits

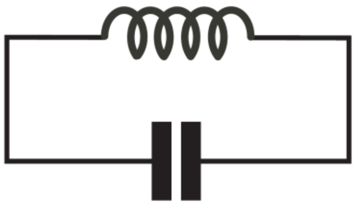


Neutral atoms

Boston Consulting Group – Nov 2018

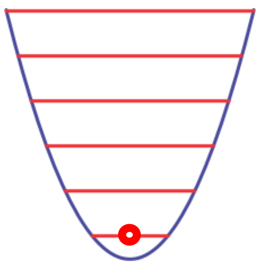
Superconducting circuits

LC circuit



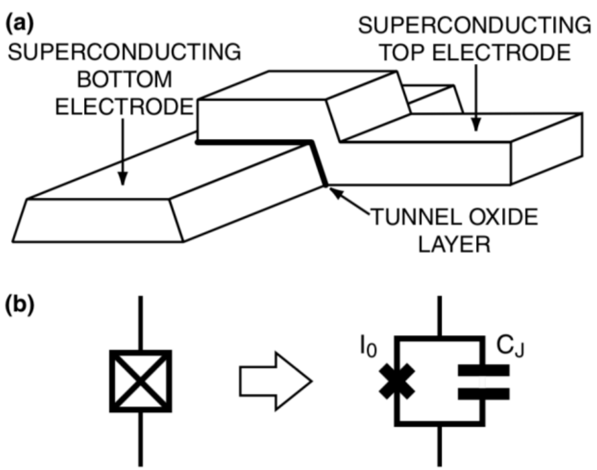
$$\omega_0 = \frac{1}{\sqrt{LC}} \sim \text{GHz}$$

Harmonic oscillator

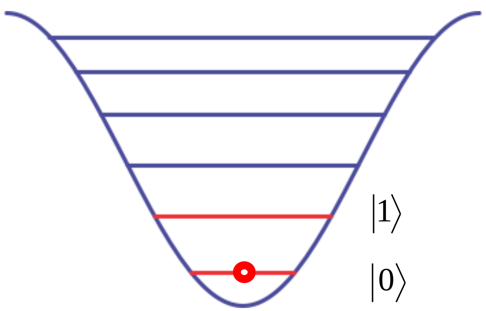


Equidistant energy levels
No quantum bit

Non linear component



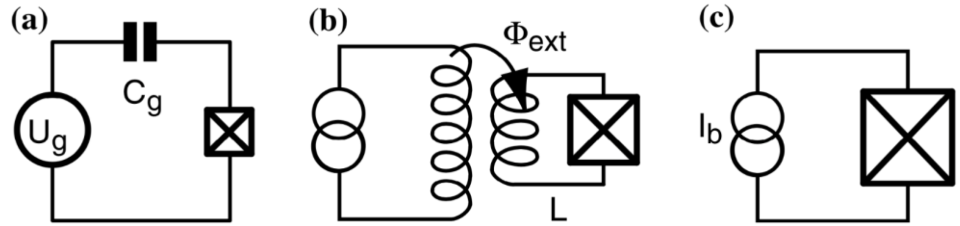
Josephson junction



$$T = 50\ \text{mK} < \hbar\omega_0 / k_B \approx 250\ \text{mK}$$

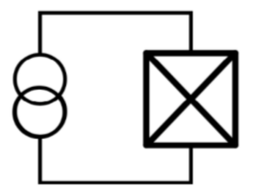
To know more : Devoret and Martinis - Quantum Information Processing, Vol. 3, Nos. 1–5, October 2004 (© 2004)

Superconducting circuits

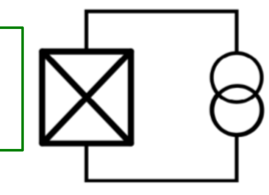


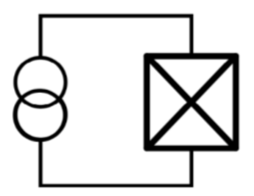
charge qubit   flux qubit   phase qubit

Coupling two qubits:

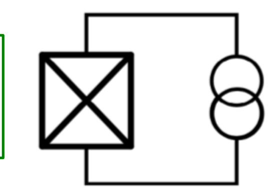


Electrical coupling
(circuit)





Quantum bus
(microwave photons)



Some chip example

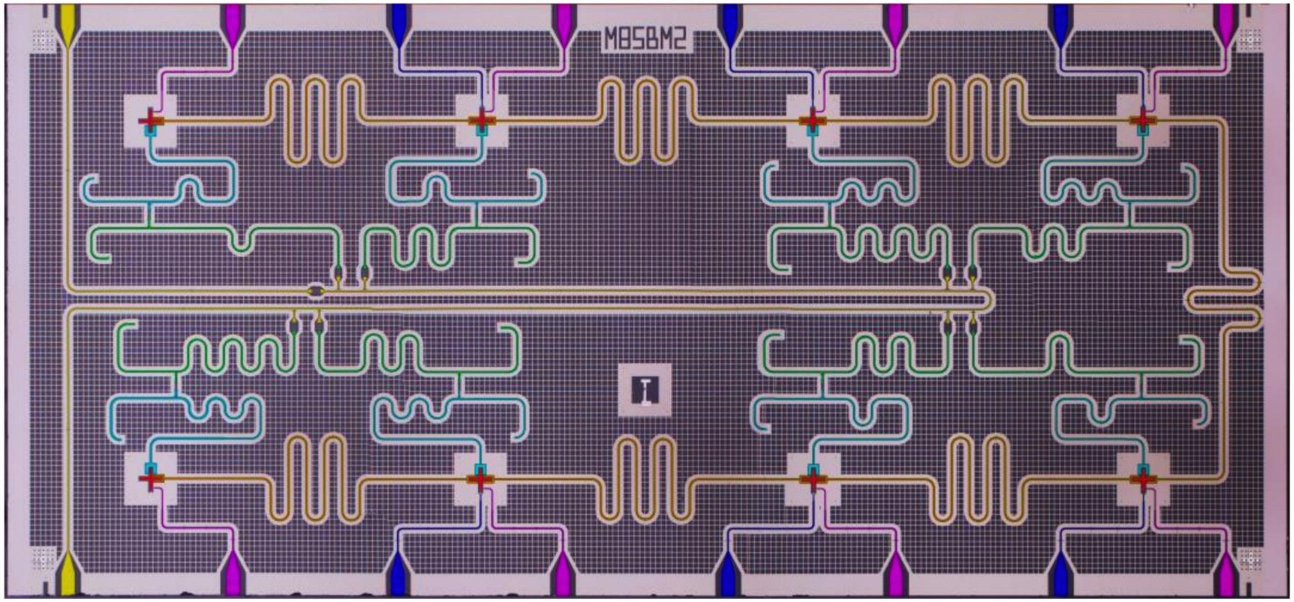


Figure 3: False-coloured image of an 8-qubit superconducting quantum processor fabricated at ETH Zurich. All eight qubits (red) are measured using a common readout line (yellow), by coupling each qubit (red) to a pair of readout resonator (cyan) and Purcell filter (green). Qubit control is enabled by individual charge lines (purple) and flux lines (blue). Coupling between nearest neighbour qubits is mediated by bus resonators (orange).

arXiv 1712.03773

Superconducting circuits

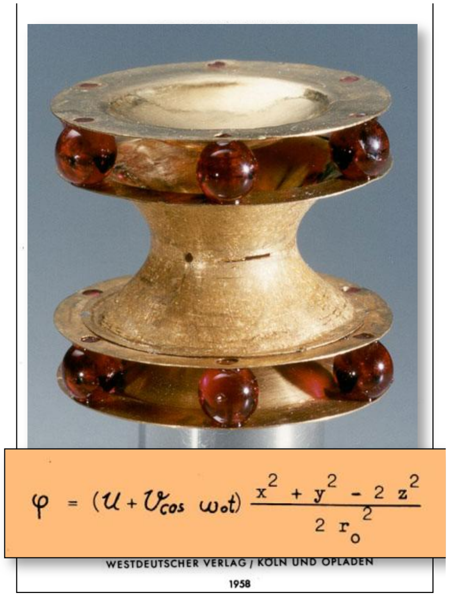
Assests:

- Electronic based technology
- On chip – scalable
- Many degrees of freedom
- Only electronics – very flexible

Some challenges:

- Wiring
- Footprint
- Cooling down
- Noise: charges, magnetic fluctuations
- Cross talk

Trapped ions

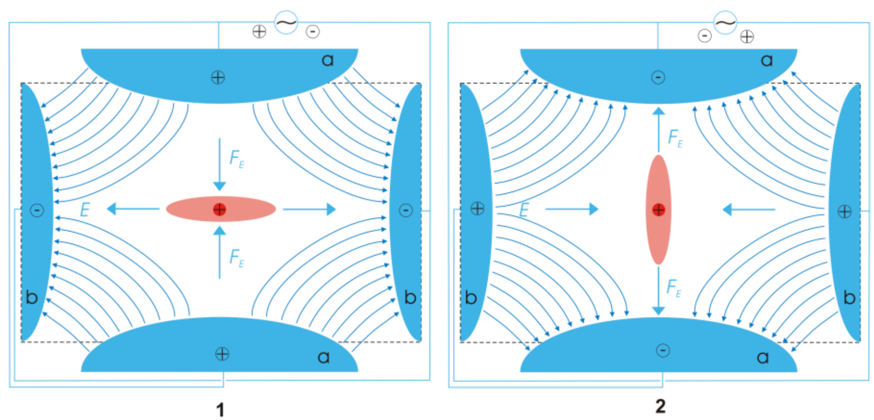


$$\varphi = (\mathcal{U} + \mathcal{V} \cos \omega_0 t)\,\frac{x^2 + y^2 - 2z^2}{2 r_0^2}$$

1989 Nobel prize

Hans G. Dehmelt and Wolfgang Paul
"for the development of the ion trap technique."

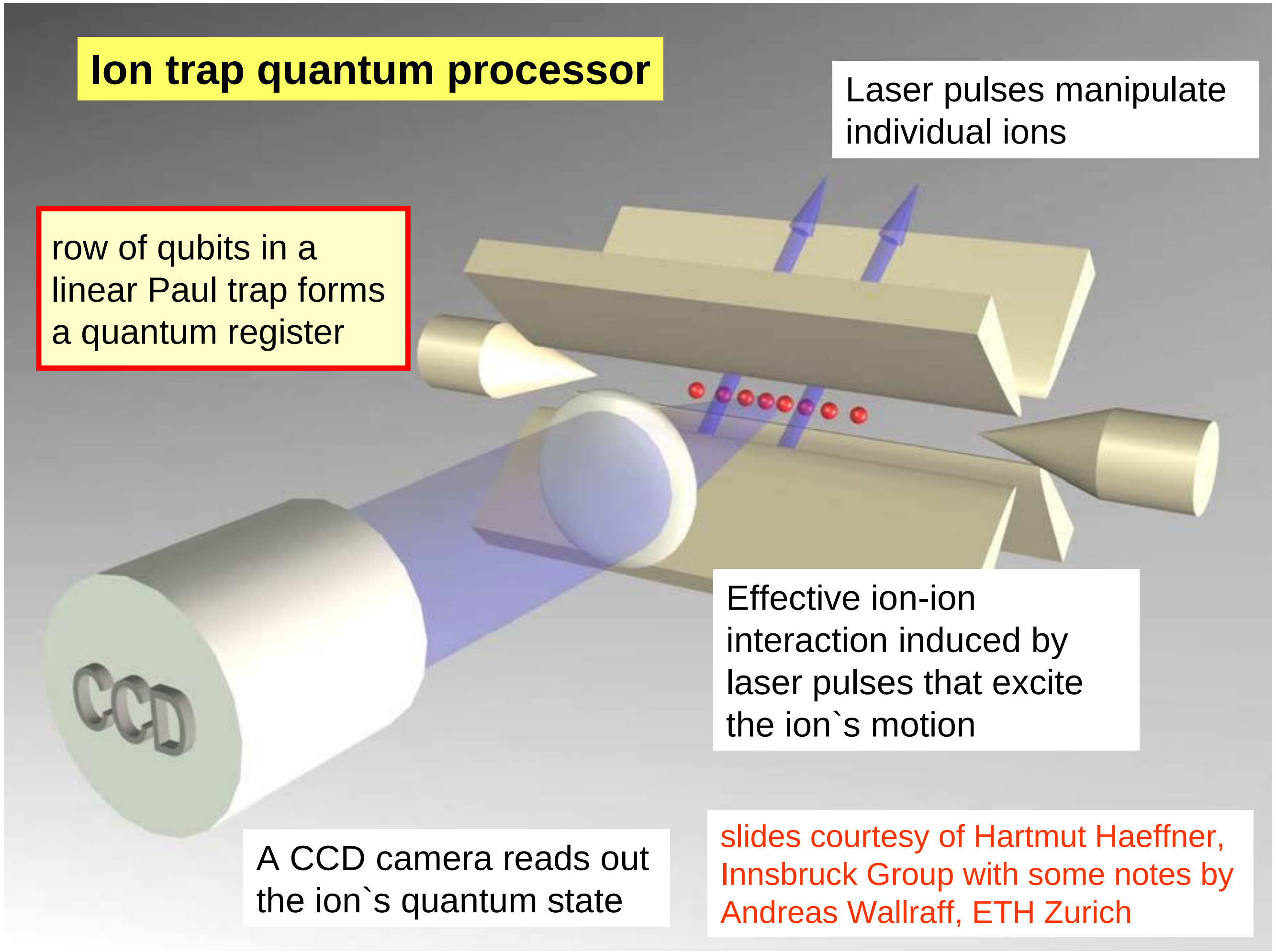
Quadrupolar trap for charged particle



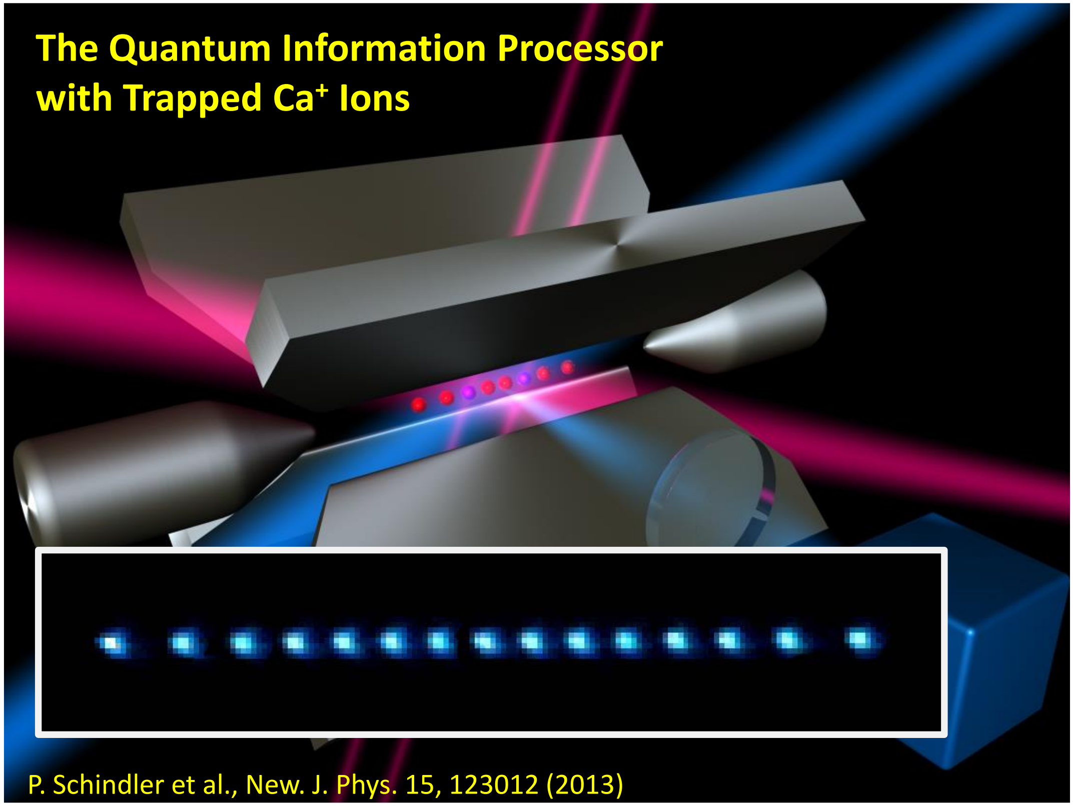
To know more : Séminaire au Collège de France – Professeur Rainer Blatt – Insbruck University- 10 mars 2015

Vidéo et transparents en ligne: https://www.college-de-france.fr/site/serge-haroche/seminar-2015-03-10-11h00.htm

Trapped ions



Trapped ions



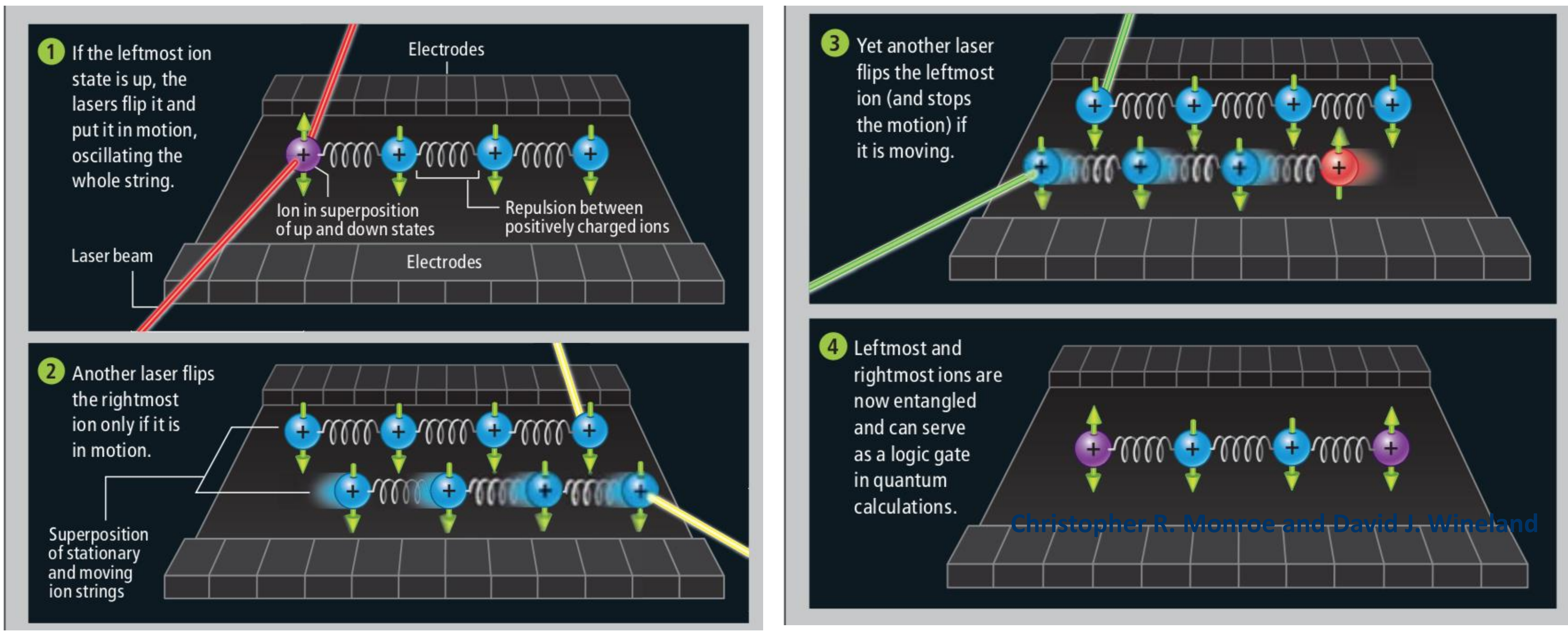
Trapped ions

Two-qubit gates

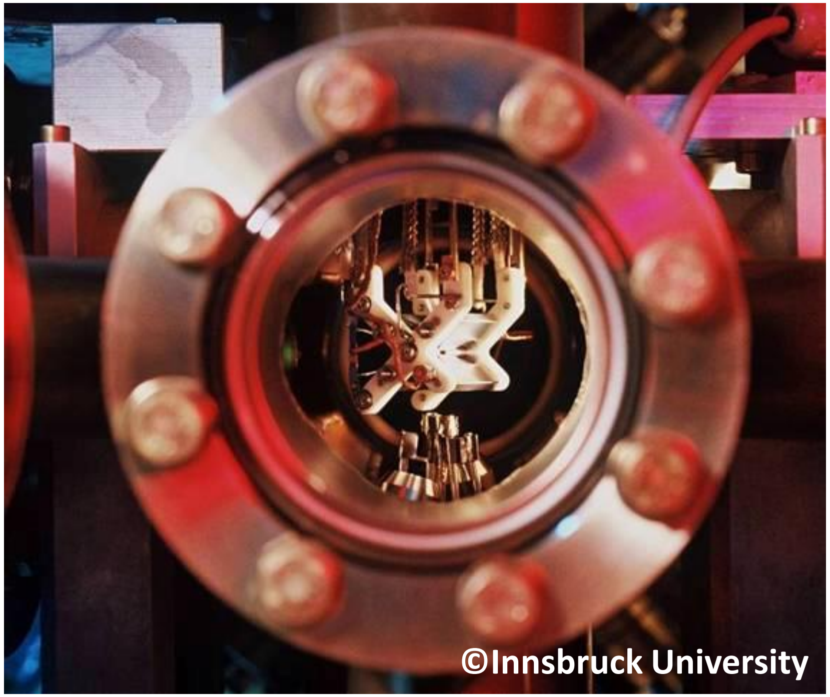
VOLUME 74, NUMBER 20 PHYSICAL REVIEW LETTERS 15 MAY 1995

Quantum Computations with Cold Trapped Ions

J. I. Cirac and P. Zoller*
Institut für Theoretische Physik, Universiät Innsbruck, Technikerstrasse 25, A-6020 Innsbruck, Austria



Trapped ions



Assests:

- Low decoherence
- Excellent connectivity
- Room temperature (except for vacuum)

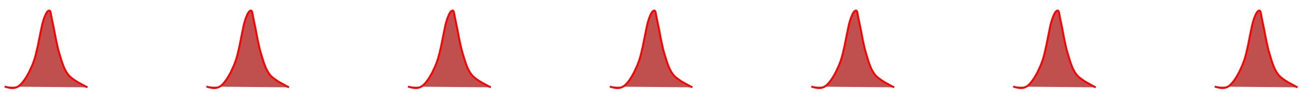
Some challenges:

- Miniaturizarion
- Increasing the qubit number

Photons

Single photon qubit

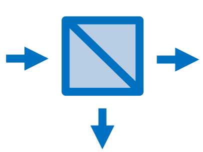
On demand deterministic single photon source



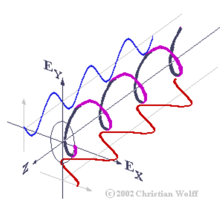
$|1\rangle$ $|1\rangle$ $|1\rangle$ $|1\rangle$ $|1\rangle$ $|1\rangle$ $|1\rangle$

Many degrees of freedom - Hyperencoding

- ✓ **Path**

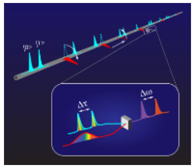


- ✓ **Polarization**

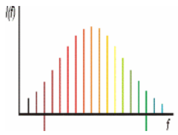


- ✓ **OAM**

- ✓ **Time**



- ✓ **Energy**



- ✓ **Photon number**

$\sqrt{p_0}|0_a\rangle + \sqrt{p_1}e^{i\alpha_1}|1_a\rangle$

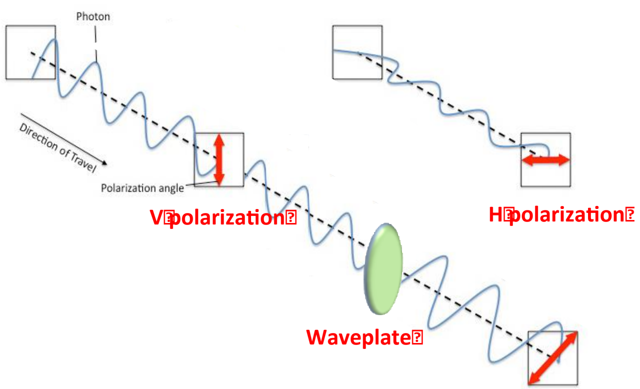
Photons

No decoherence

Photons are non-interacting particles in vacuum

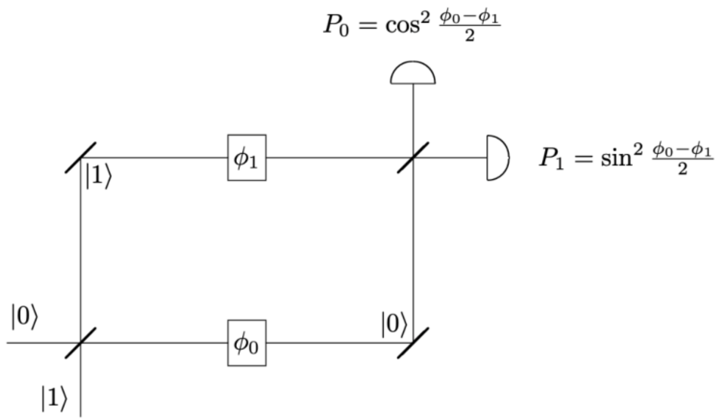
Single qubit gates

Polarization encoding



$$|Y\rangle = a|H\rangle + be^{ij}|V\rangle$$

Path encoding



$$|Y\rangle = a|a\rangle + be^{ij}|b\rangle$$

Two quantum bit gates ?? (the great challenge)

A scheme for efficient quantum computation with linear optics

E. Knill*, R. Laflamme* & G. J. Milburn†

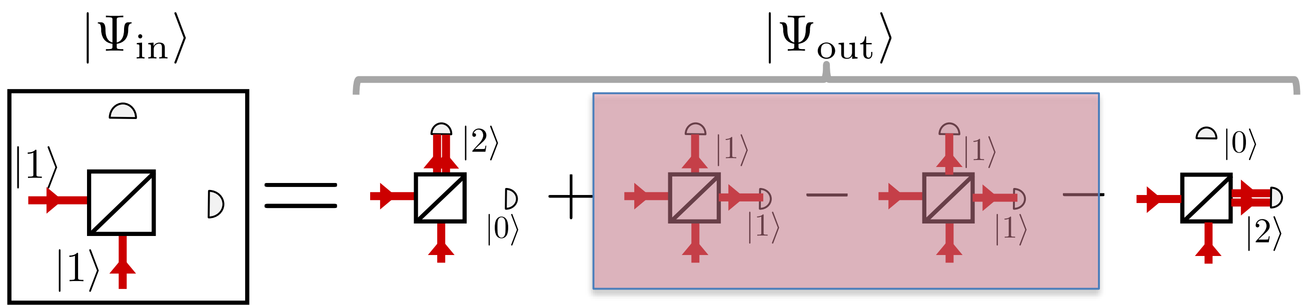
* *Los Alamos National Laboratory, MS B265, Los Alamos, New Mexico 87545, USA*
† *Centre for Quantum Computer Technology, University of Queensland, St. Lucia, Australia*

Quantum computers promise to increase greatly the efficiency of solving problems such as factoring large integers, combinatorial optimization and quantum physics simulation. One of the greatest challenges now is to implement the basic quantum-computational elements in a physical system and to demonstrate that they can be reliably and scalably controlled. One of the earliest proposals for quantum computation is based on implementing a quantum bit with two optical modes containing one photon. The proposal is appealing because of the ease with which photon interference can be observed. Until now, it suffered from the requirement for non-linear couplings between optical modes containing few photons. Here we show that efficient quantum computation is possible using only beam splitters, phase shifters, single photon sources and photo-detectors. Our methods exploit feedback from photo-detectors and are robust against errors from photon loss and detector inefficiency. The basic elements are accessible to experimental investigation with current technology.

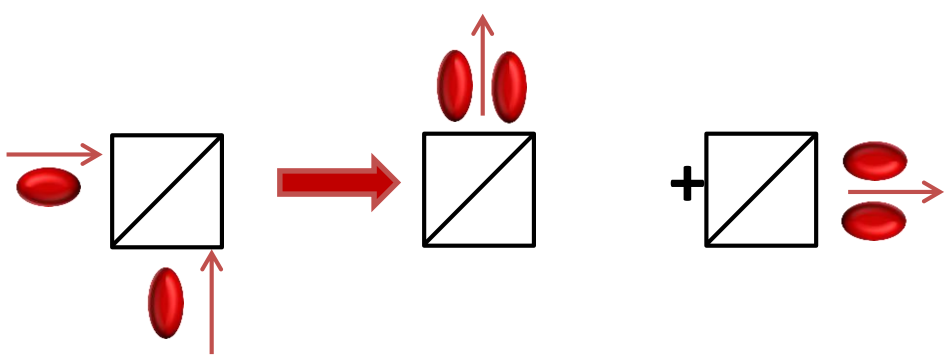
Knill, E.; Laflamme, R.; Milburn, G. J. Nature (2001)

Linear optical quantum computing

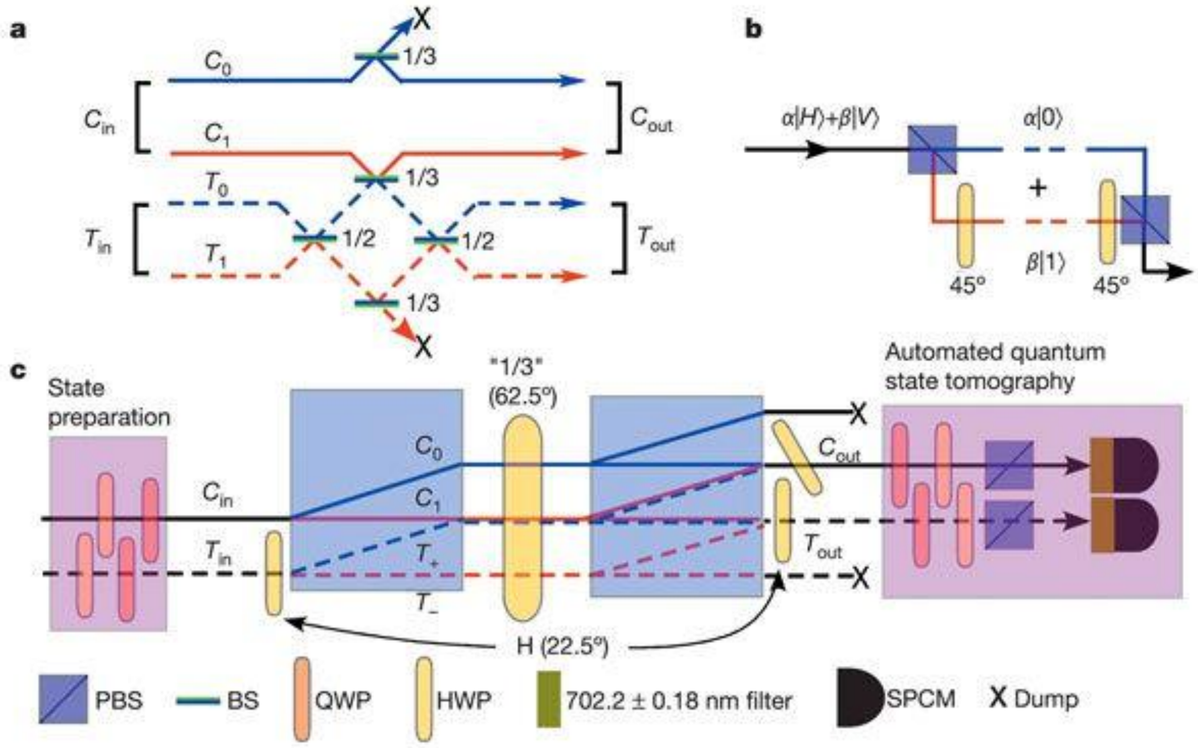
Exploit the quantum interference



$$|\Psi_{in}\rangle = |1_a, 1_b\rangle \Rightarrow |\Psi_{out}\rangle = \frac{1}{\sqrt{2}}\left(|2_c, 0_d\rangle - |0_c, 2_d\rangle\right)$$

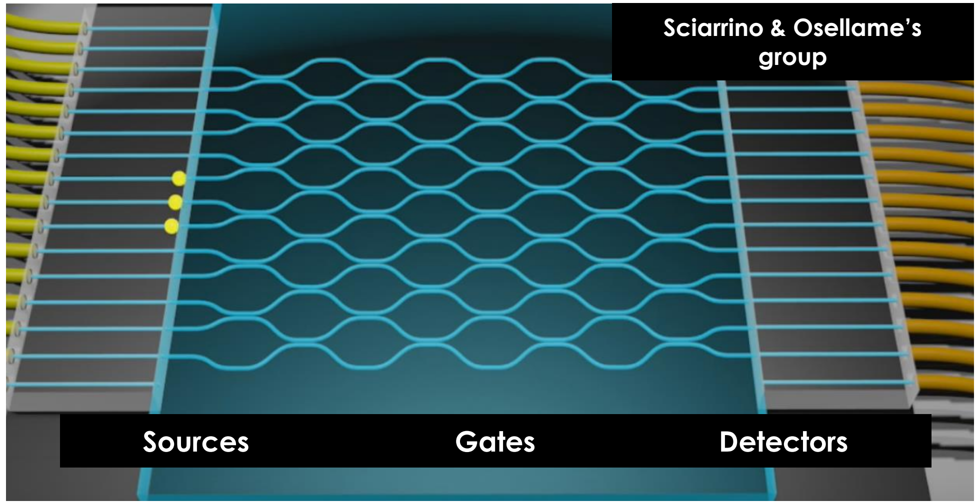


Example of 2-photon CNOT gate



Nature volume 426, 264 (2003)

Optical Quantum computer architecture



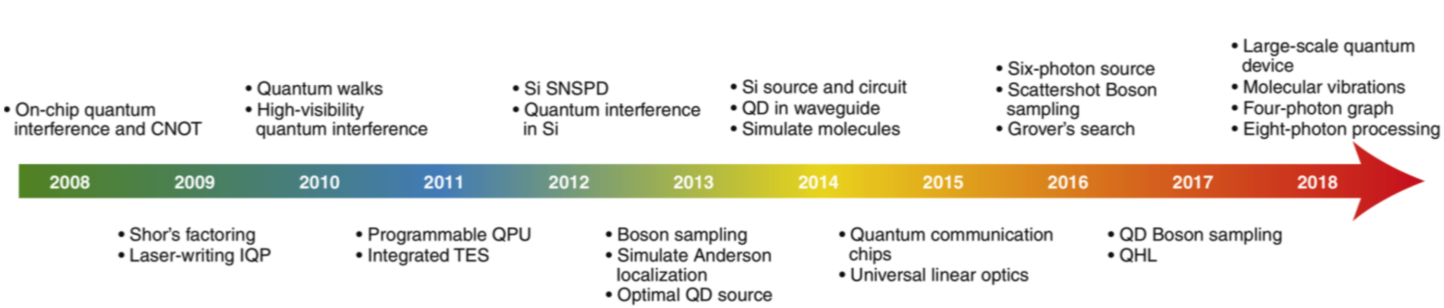
nature photonics

REVIEW ARTICLE

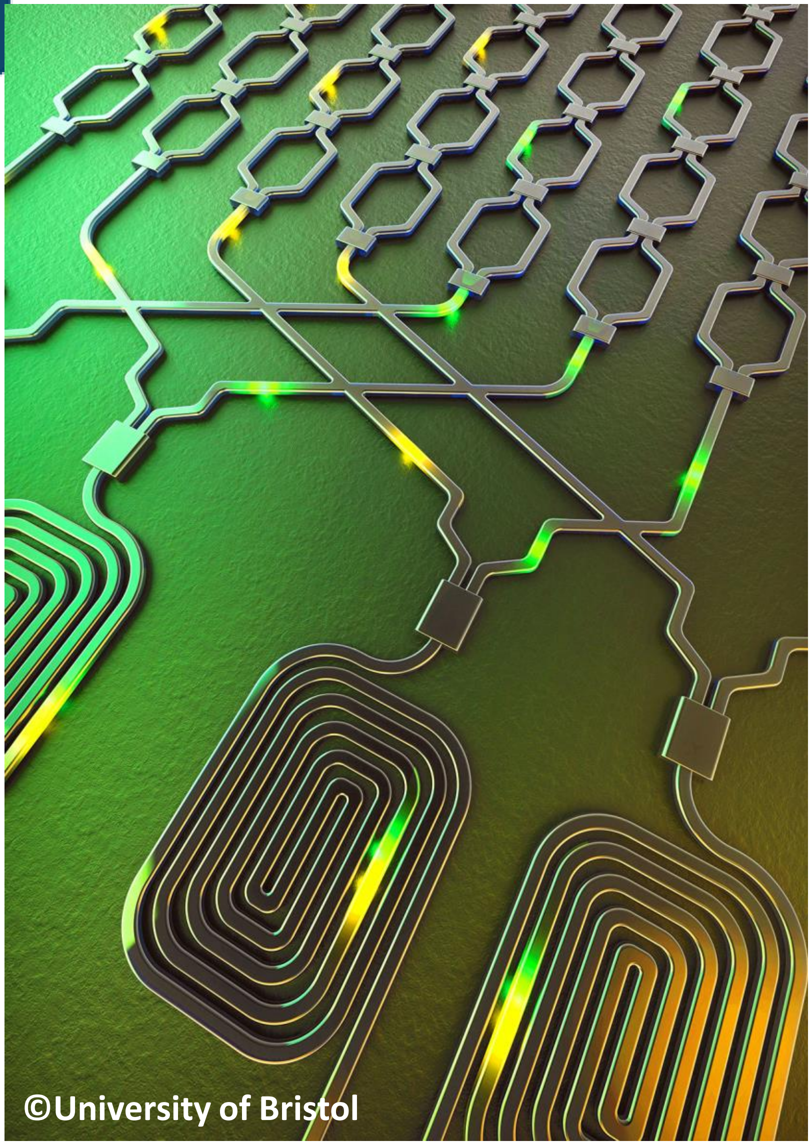
https://doi.org/10.1038/s41566-019-0532-1

Integrated photonic quantum technologies

Jianwei Wang[1], Fabio Sciarrino[2], Anthony Laing[3] and Mark G. Thompson[3*]



Photons



Assests:

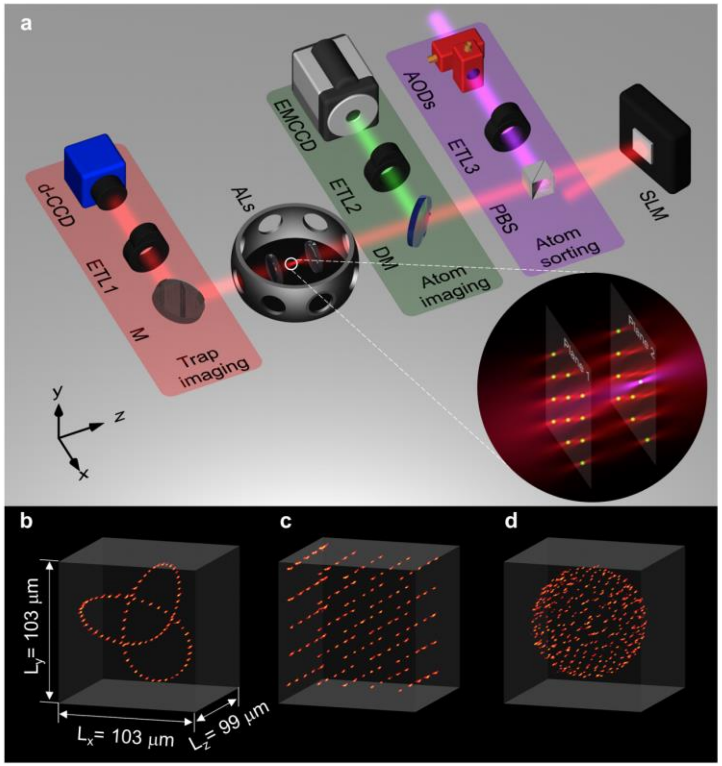
- No decoherence
- Good connectivity
- Room temperature processing
- Naturally connect to a quantum network

Some challenges:

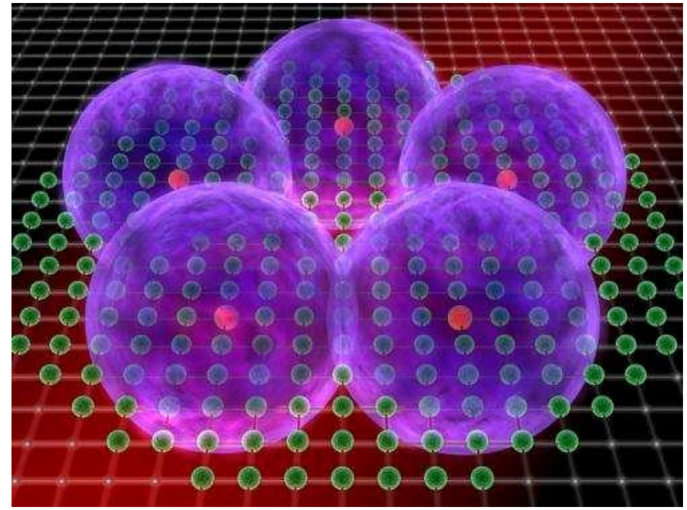
- Very inefficient 2-qubit gates
- Efficient light sources

Rydberg atoms

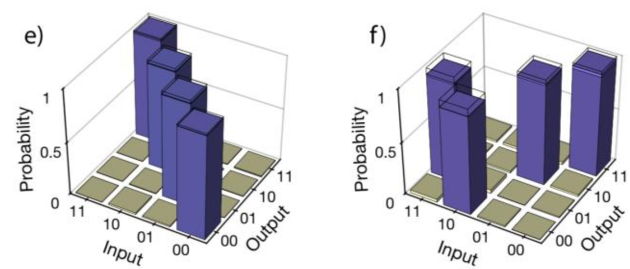
Synthetic three-dimensional atomic structures assembled atom by atom



Nature 561, 79 (2018)



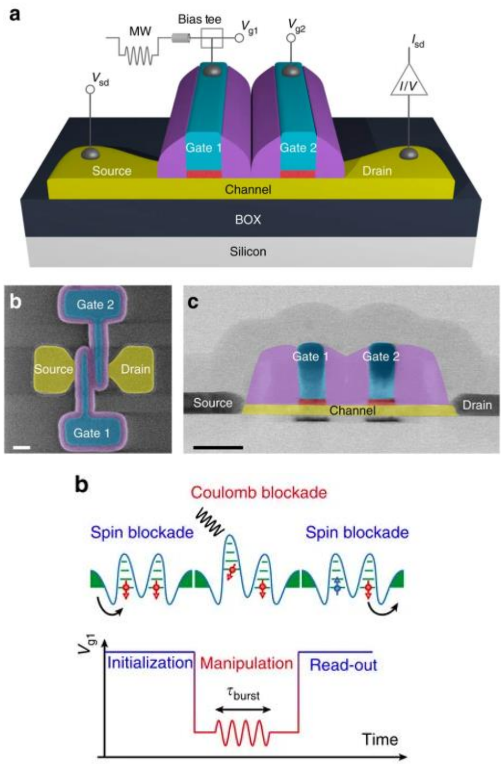
Credit: MPQ Garching
Rydberg mediated interactions



Parallel implementation of high-fidelity multi-qubit gates with neutral atoms

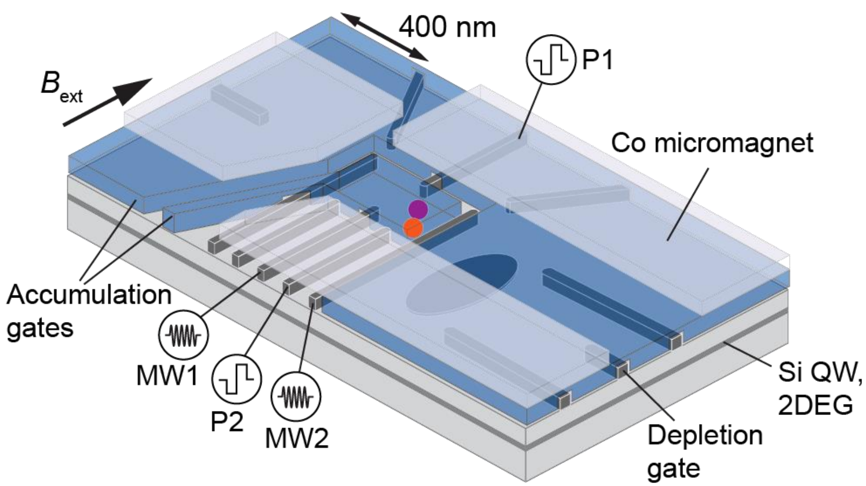
arXiv:1908.06101

Electron spin in silicium



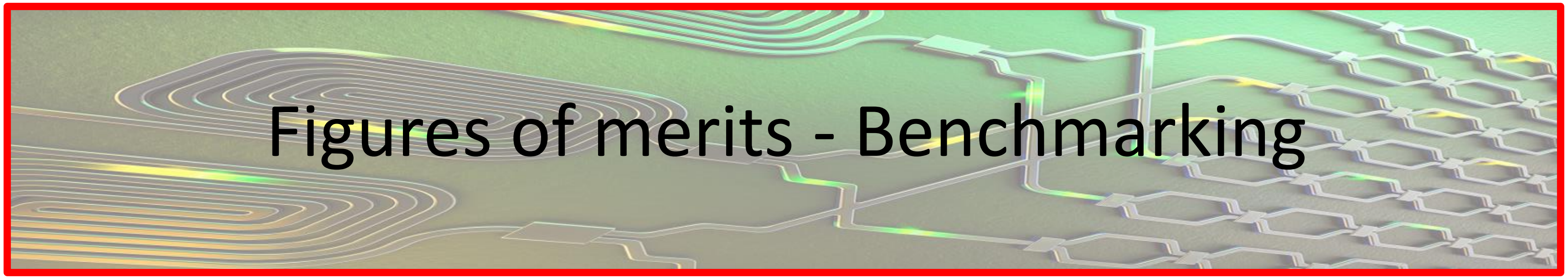
Nature Communications 7, 13575 (2016)

A programmable two-qubit quantum processor in silicon



Nature 555, 633 (2018)

Figures of merits - Benchmarking

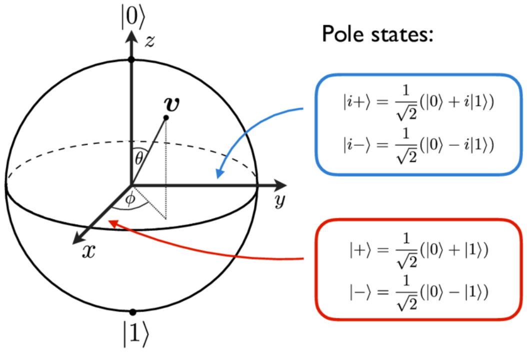


Figures of merit

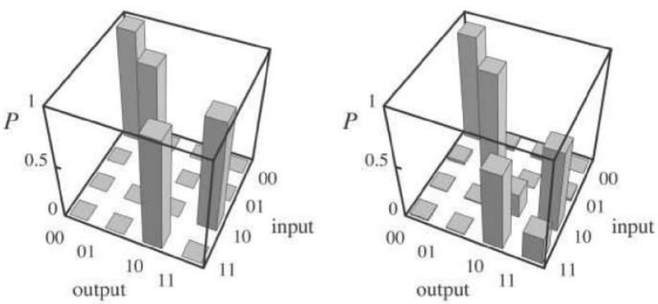
Number of qubits

Fabricated
versus
measured
Number of quantum bits

Single qubit gate errors



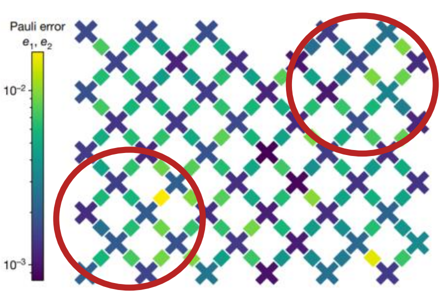
Two-qubit gate errors



Nature 426, 264 (2003)

Connectivity

Parallelisation capabilities



Google sycomore

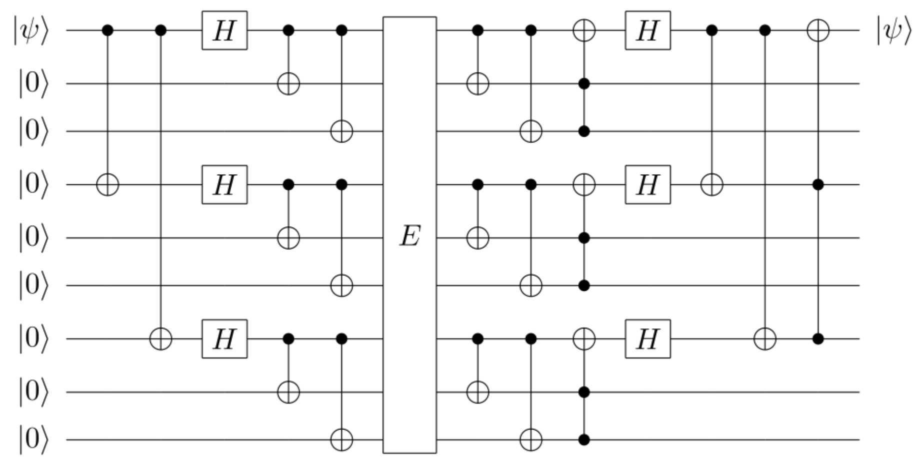
Quantum depth

Ratio between coherence time and gate time

time

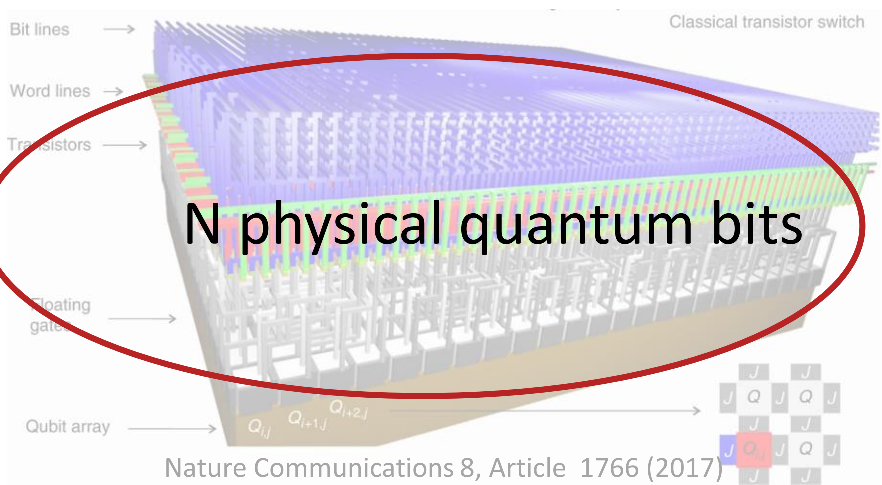
Physical versus logical quantum bits

Shor code for arbitrary single-qubit error correction.



Error correction:

- Additional quantum bits
- Additional gates



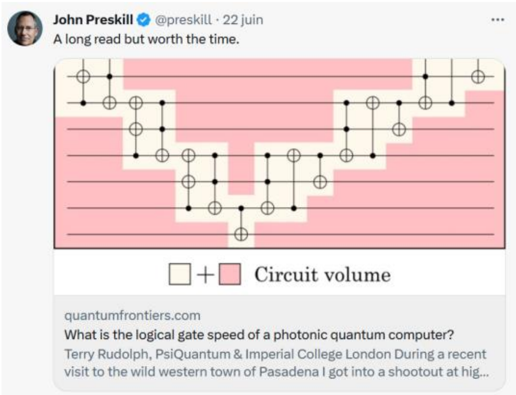
N physical quantum bits → 1 logical quantum bit

Nature Communications 8, Article 1766 (2017)

Quantum advantage

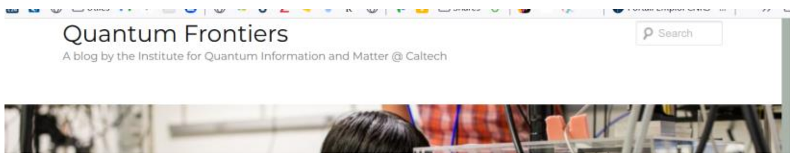
Define intermediate milestones

~~Quantum Supremacy~~ → Quantum Advantage



…run an algorithm on a quantum computer which solves problems with a super-polynomial speedup relative to classical computers. (irrespective of the usefulness of the problem)

John Preskill,
Caltech Solvay Conference
19 October 2011



https://quantumfrontiers.com/author/preskill/

« On entangled evening» song

A circuit that cold
Is worth more than gold
For qubits within it.
Will do as they're told.

Then our quantum goods
Will work as they should
Solving the problems
No old gadget could!

NISQ computing era = Noisy Intermediate-Scale Quantum

Introduced by John Preskill in 2018

Quantum simulation, quantum chemistry
Optimization problems, search problems…

Boson sampling

Scott Aaronson


Shtetl-Optimized
The Blog of Scott Aaronson
If you take nothing else from this blog: quantum computers won't solve hard problems instantly by just trying all solutions in parallel.
Also, next pandemic, let's approve the vaccines faster!

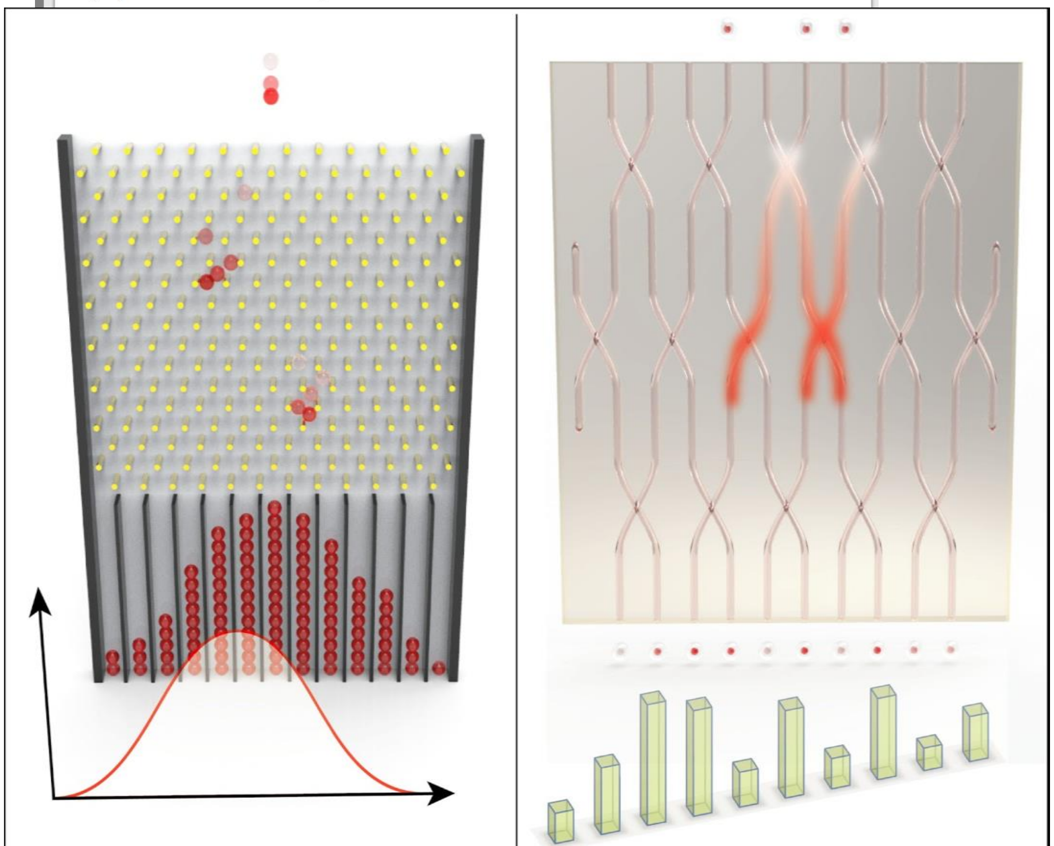
PSPACE
PostBQP
NP
BQP
P

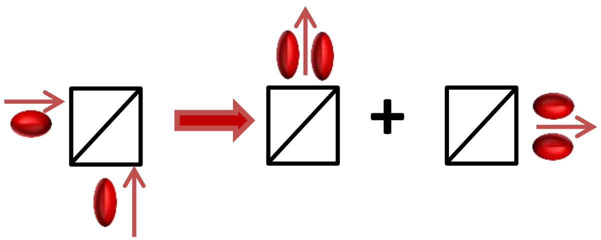
« Could GPT help with dating anxiety?

Life, blogging, and the Busy Beaver function go on »

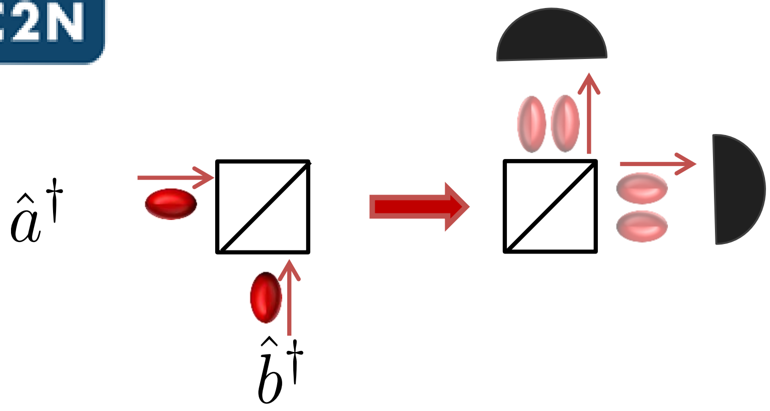
Book Review: "Quantum Supremacy" by Michio Kaku (tl;dr DO NOT BUY)

The Computational Complexity of Linear Optics
Scott Aaronson, Alex Arkhipov
arXiv:1011.3245





Boson sampling proposition



$$\text{BS}=\begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix}$$

$$\hat{a}^\dagger\hat{b}^\dagger \rightarrow c_1c_3(\hat{a}^\dagger)^2 + c_2c_4(\hat{b}^\dagger)^2 + (c_1c_4 + c_2c_3)\hat{a}^\dagger\hat{b}^\dagger$$

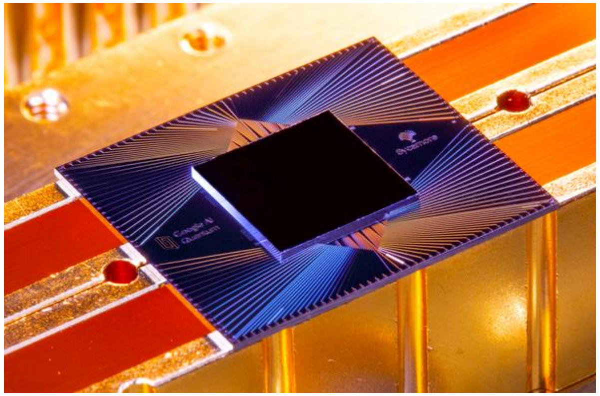
$$\text{per}\begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} = c_1c_4 + c_2c_3$$

Calculating permanents is in the N-P complexity class

Valiant, *The complexity of computing the permanent*, Theo. Comp. Scie. 8, 189 (1979)

Quantum advantage: 50 photons, 100 modes

Google technological breakthrough

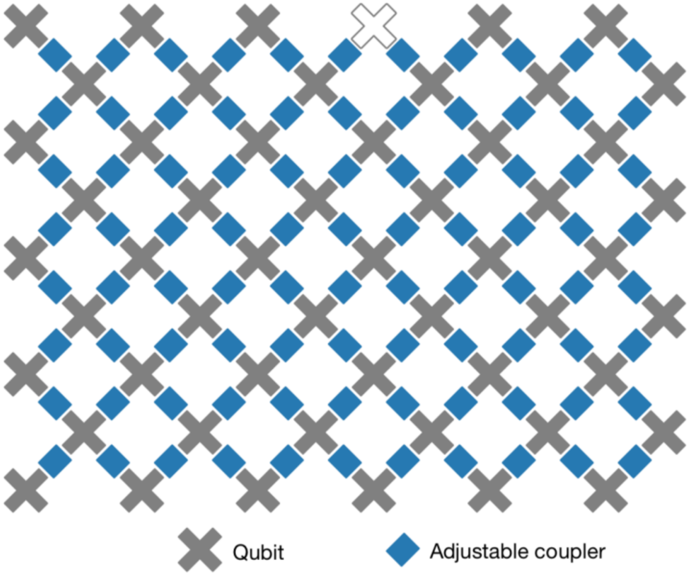


Article

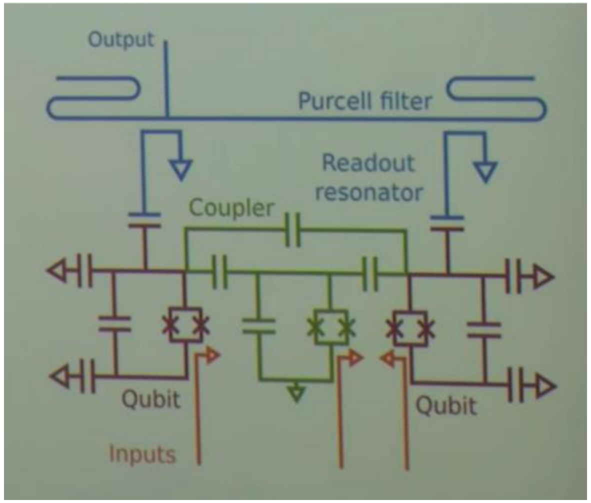
Quantum supremacy using a programmable superconducting processor

https://doi.org/10.1038/s41586-019-1666-5
Received: 22 July 2019
Accepted: 20 September 2019
Published online: 23 October 2019

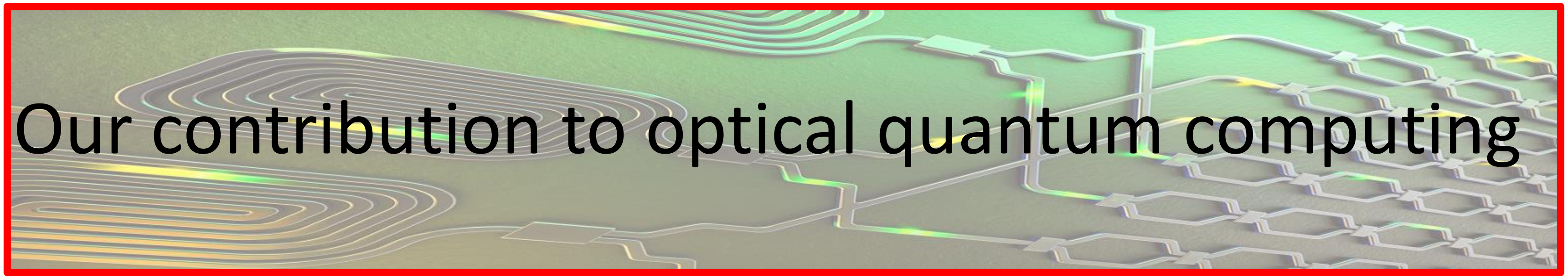
Frank Arute[1], Kunal Arya[1], Ryan Babbush[1], Dave Bacon[1], Joseph C. Bardin[1,2], Rami Barends[1], Rupak Biswas[3], Sergio Boixo[1], Fernando G. S. L. Brandao[1,4], David A. Buell[1], Brian Burkett[1], Yu Chen[1], Zijun Chen[1], Ben Chiaro[5], Roberto Collins[1], William Courtney[1], Andrew Dunsworth[1], Edward Farhi[1], Brooks Foxen[1,5], Austin Fowler[1], Craig Gidney[1], Marissa Giustina[1], Rob Graff[1], Keith Guerin[1], Steve Habegger[1], Matthew P. Harrigan[1], Michael J. Hartmann[1,6], Alan Ho[1], Markus Hoffmann[1], Trent Huang[1], Travis S. Humble[7], Sergei V. Isakov[1], Evan Jeffrey[1], Zhang Jiang[1], Dvir Kafri[1], Kostyantyn Kechedzhi[1], Julian Kelly[1], Paul V. Klimov[1], Sergey Knysh[1], Alexander Korotkov[1,8], Fedor Kostritsa[1], David Landhuis[1], Mike Lindmark[1], Erik Lucero[1], Dmitry Lyakh[9], Salvatore Mandrà[3,10], Jarrod R. McClean[1], Matthew McEwen[5], Anthony Megrant[1], Xiao Mi[1], Kristel Michielsen[11,12], Masoud Mohseni[1], Josh Mutus[1], Ofer Naaman[1], Matthew Neeley[1], Charles Neill[1], Murphy Yuezhen Niu[1], Eric Ostby[1], Andre Petukhov[1], John C. Platt[1], Chris Quintana[1], Eleanor G. Rieffel[3], Pedram Roushan[1], Nicholas C. Rubin[1], Daniel Sank[1], Kevin J. Satzinger[1], Vadim Smelyanskiy[1], Kevin J. Sung[1,13], Matthew D. Trevithick[1], Amit Vainsencher[1], Benjamin Villalonga[1,14], Theodore White[1], Z. Jamie Yao[1], Ping Yeh[1], Adam Zalcman[1], Hartmut Neven[1] & John M. Martinis[1,5*]



53 qubits and 86 adjustable couplers.

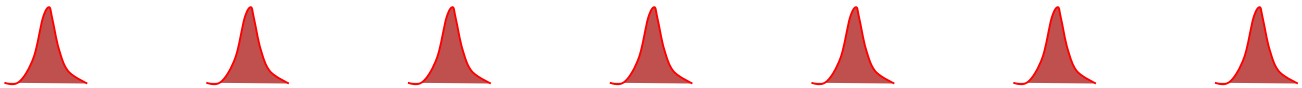


Nature 574, 505 (2019)


Our contribution to optical quantum computing

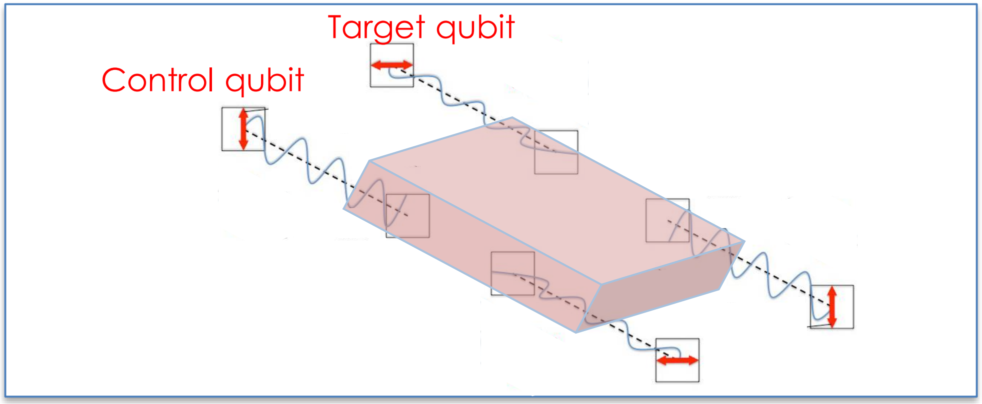
Challenges

On demand deterministic single photon source

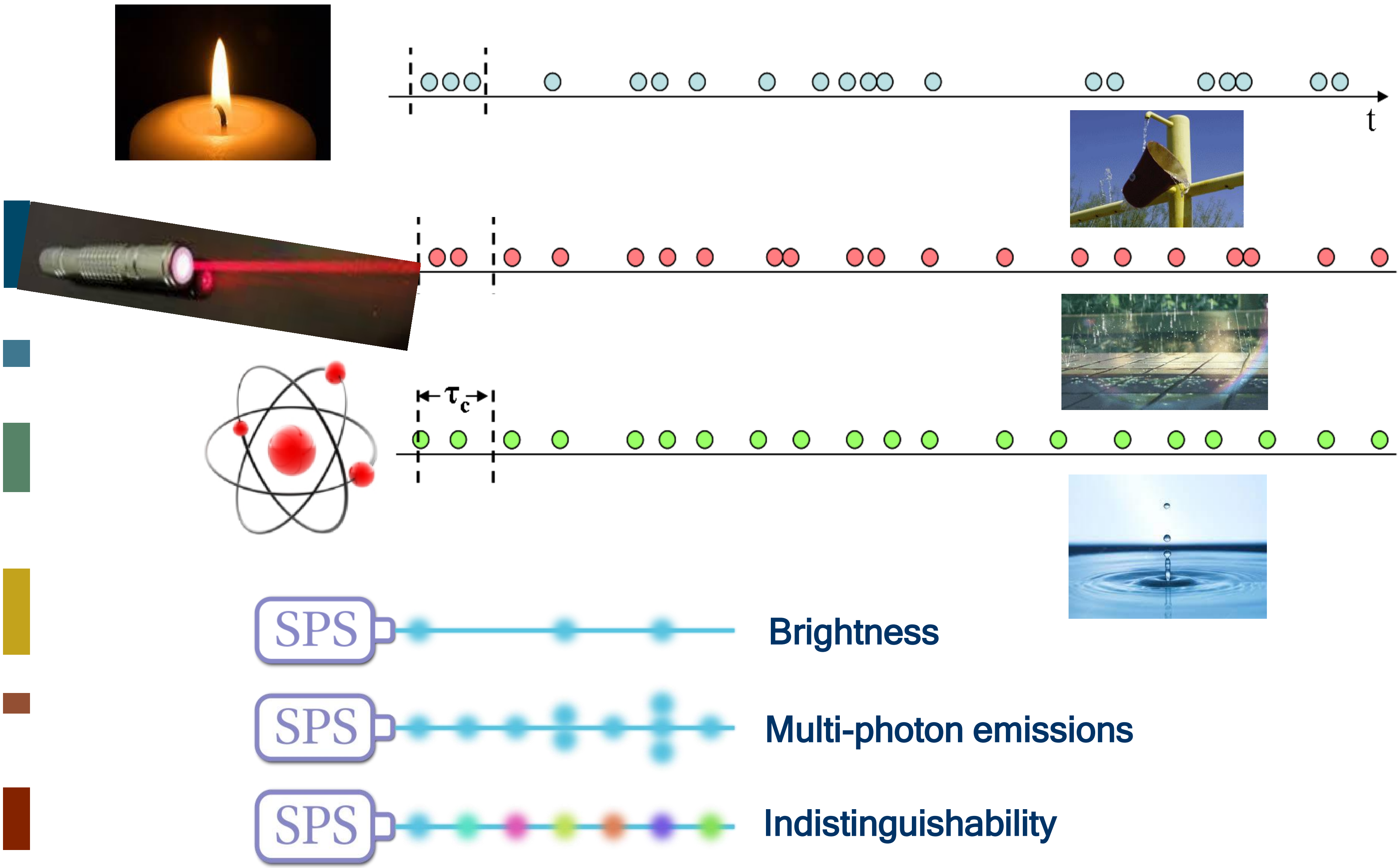


$$|1\rangle \quad |1\rangle \quad |1\rangle \quad |1\rangle \quad |1\rangle \quad |1\rangle \quad |1\rangle$$

Efficient photon-photon gates

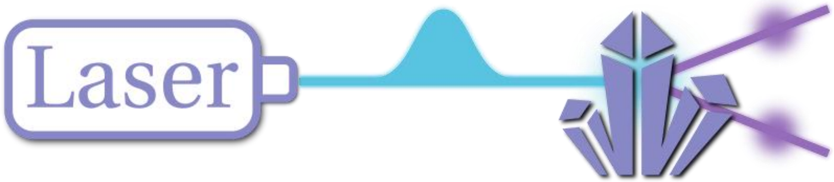


Single Photon Source SPS



Brightness of SPS

Parametric source (SPDC, SFWM…)



Brightness $\approx 1\ \%$

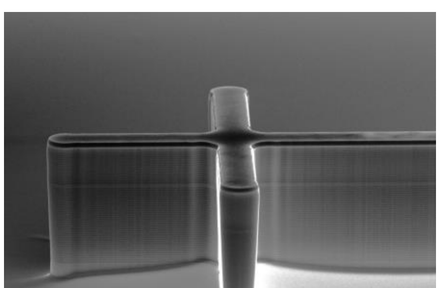
At low pump power ($|\eta| \ll 1$) :

$$\begin{aligned} |\psi\rangle &= (1-|\eta|^2/2)\,|0_s,0_i\rangle + \eta\,|1_s,1_i\rangle + \eta^2\,|2_s,2_i\rangle \\ &\approx 1\,|0_s,0_i\rangle + \eta\,|1_s,1_i\rangle + \eta^2\,|2_s,2_i\rangle \end{aligned}$$

Quantum dot in a cavity

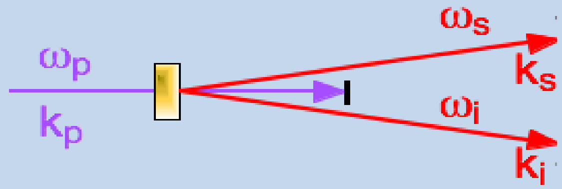
Brightness $\approx 50\ \%$ **(with current source)**

In theory, $100\ \%$ **is possible.**

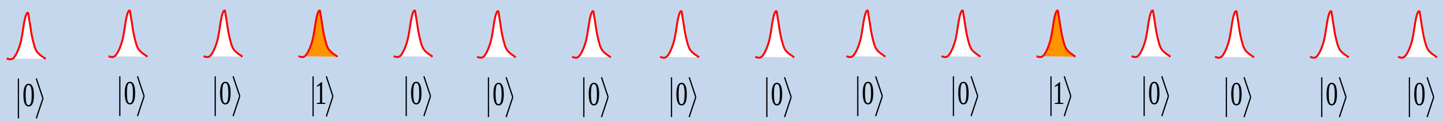


Recent / Current limitations

Highly inefficient photon sources

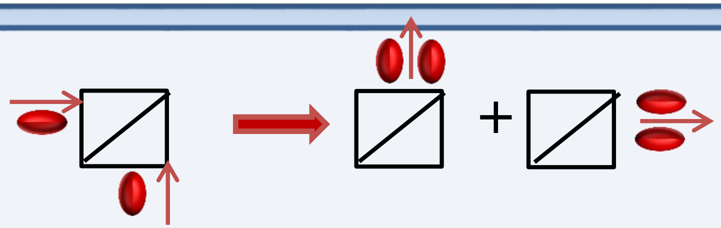


Heralded single photon source



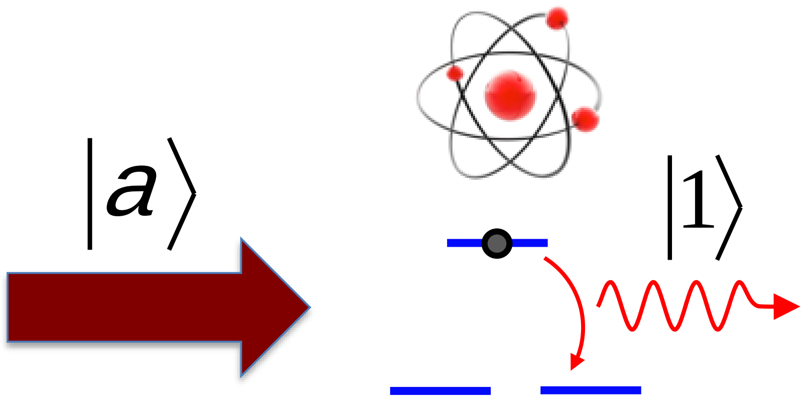
Probability to have 1 photon per pulse < 1%

<50% efficient photon-photon gates



quantum interference of identical particles + detectors

Efficient source and gate using a single atom



Kimble, Dagenais and Mandel, *Phys. Rev. Lett. 39 691 (1977)*

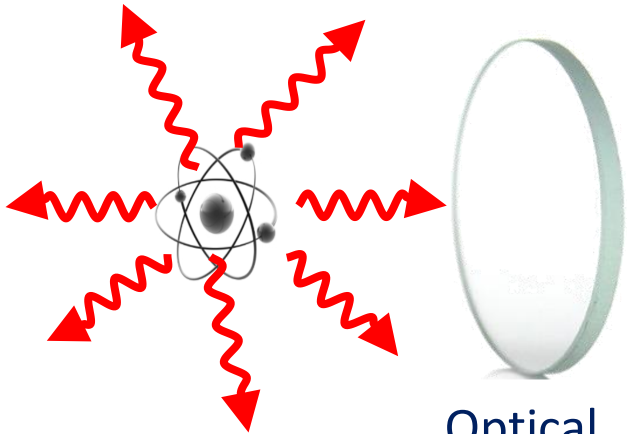
Grangier, Roger, Aspect, *Europhys. Lett 1 173 (1986)*

A single atom can only scatter/emit one photon at a time

True single photon source

Photon-photon gates

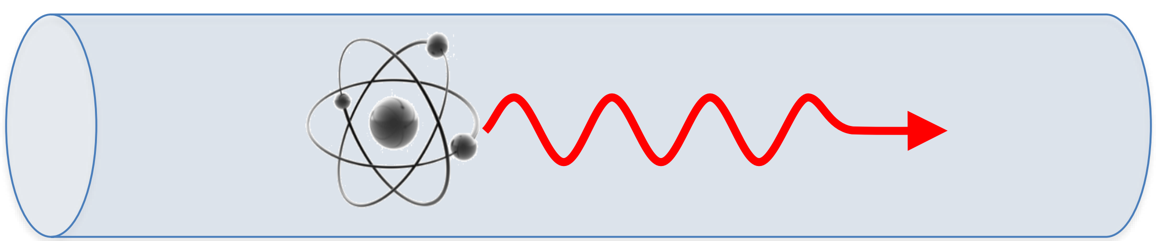
Atom-light interface



Optical lense

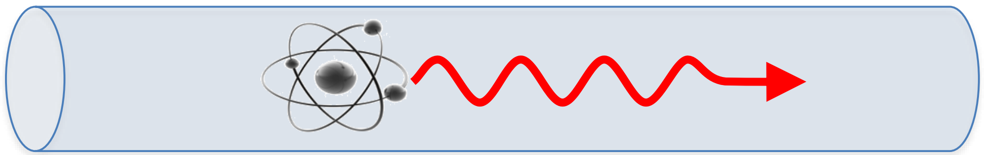
Single atom: point emitter
Isotopric emission

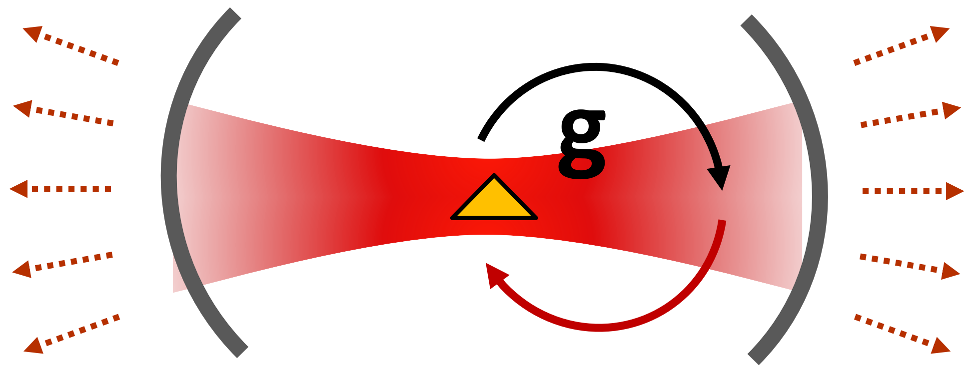
Atom coupled to a single optical mode



Atom emitting in a single direction: CQED

Atom coupled to a single optical mode





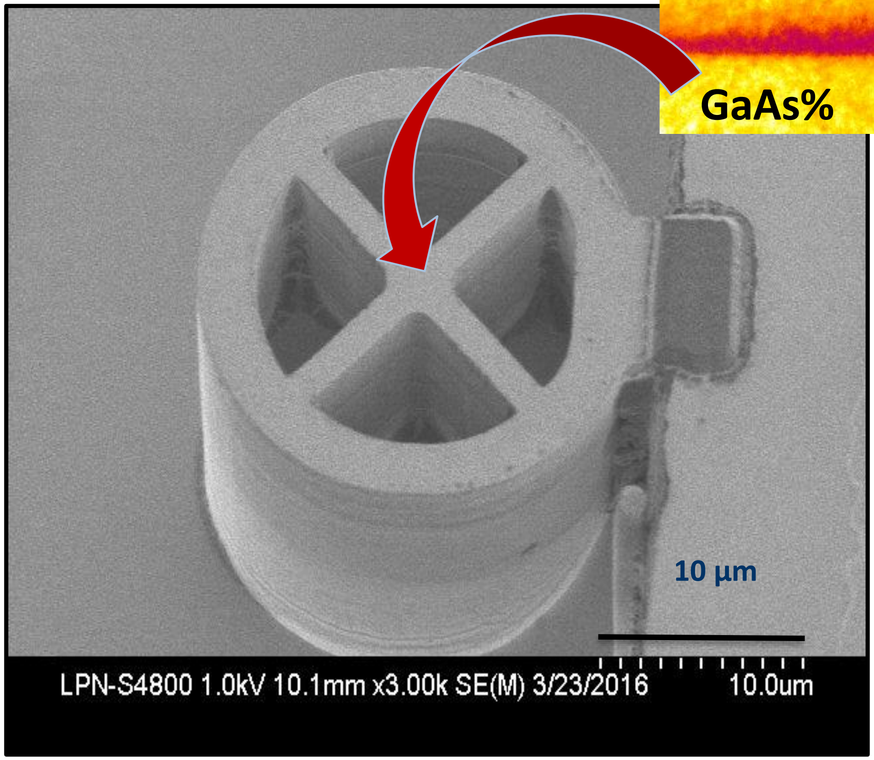
Accelerating spontaneous emission in 1 direction by factor F_p

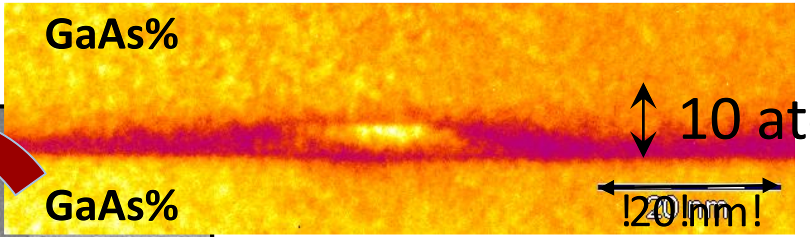
Mode coupling

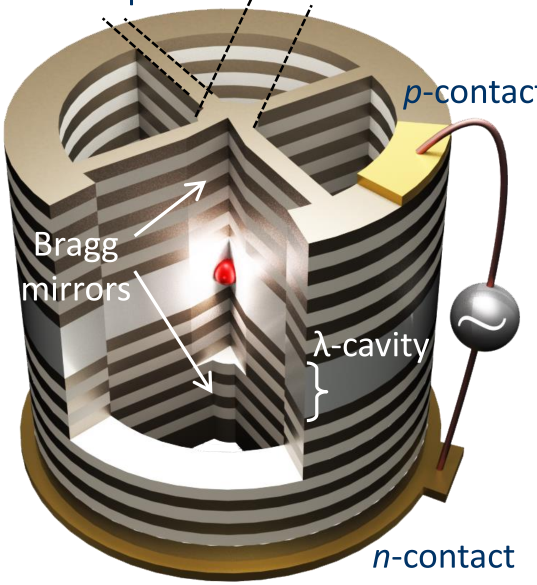
$$\beta = \frac{F_P}{F_P + 1}$$

Our implementation

Semiconductor quantum dot





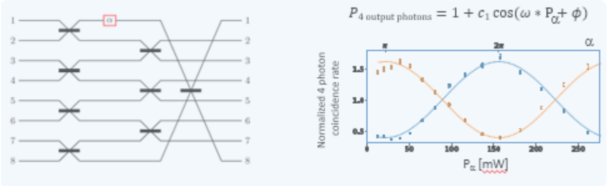


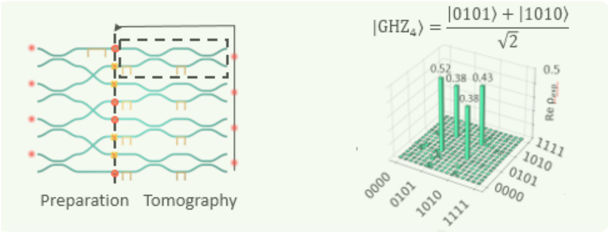
Nowak et al, Nat. Com 2014

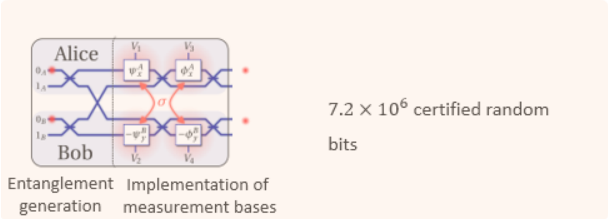
- **State-of-the-art optical circuits for NISQ/MBQC/QT/Saving the world, certification**

- **High-fidelity, high-rate , highest standard of security**

- **Implementation of protocols : RNG, 4-partite quantum secret sharing**





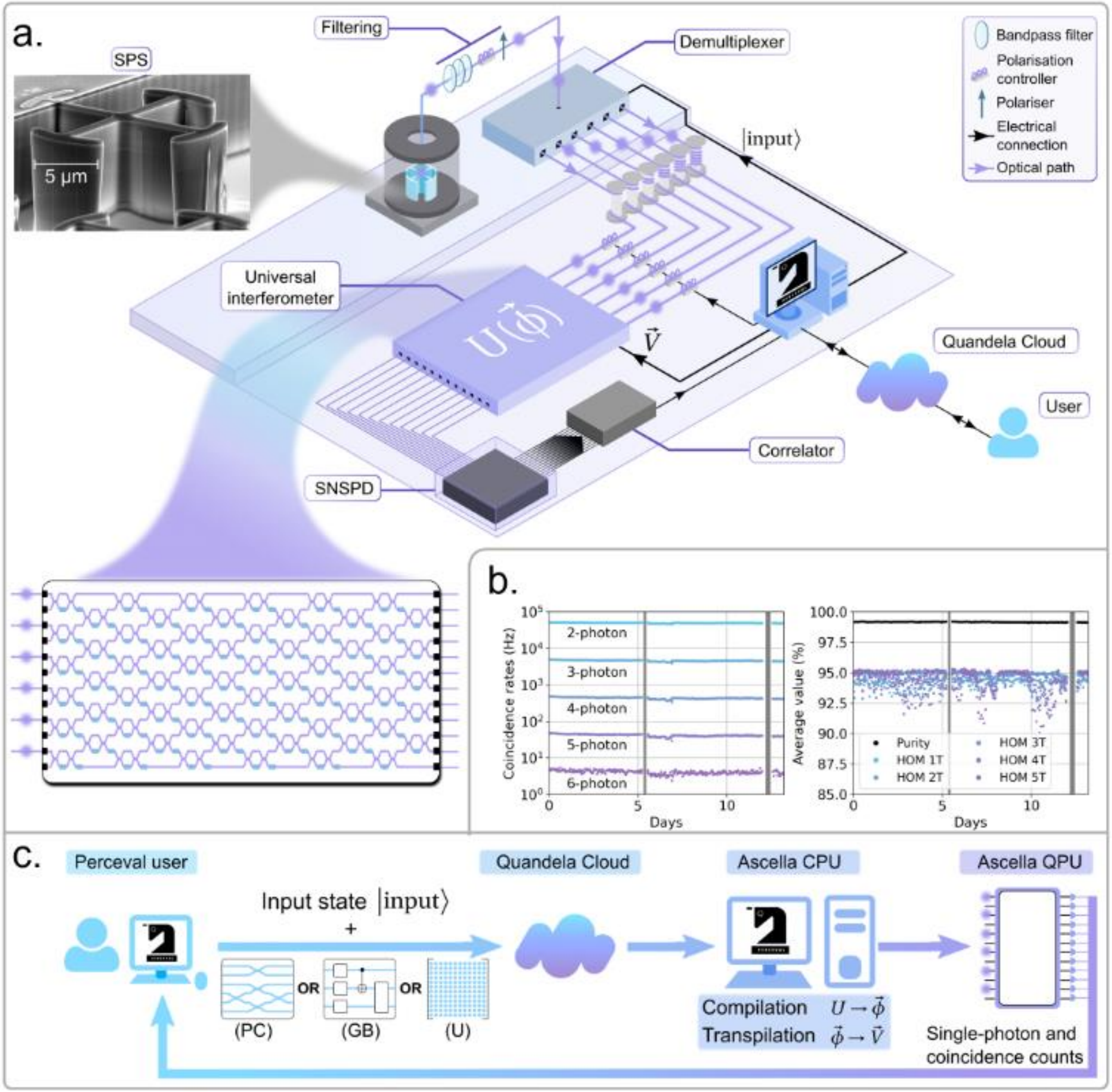


PRX 2022 ArXiv:2201.13333

Arxiv : 2301.03536

Arxiv : 2211.15626

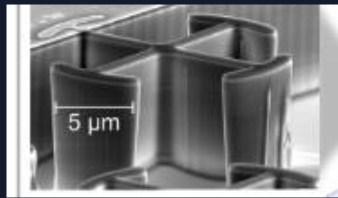
Architecture



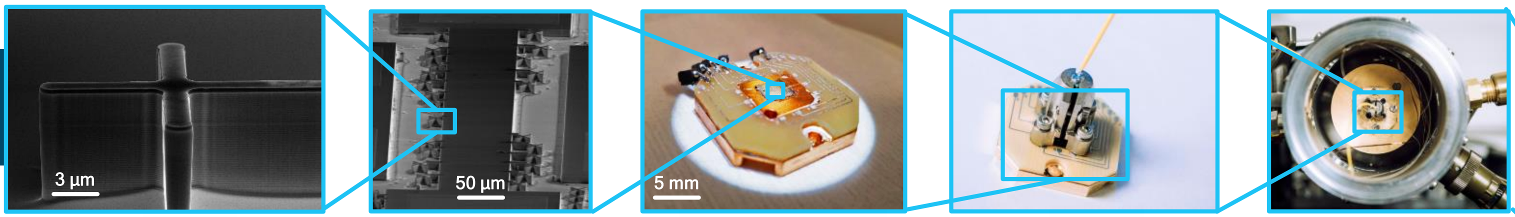
Stability

Magic

arxiv :2306.00874



Source to product



Qubit generator (identical footprint for single-photons or entangled photons)

Chip set showing multiple qubit generators

Packaged device (eDelight)

Patented fiber-pigtailed eDelight device

Compact cryogenic system

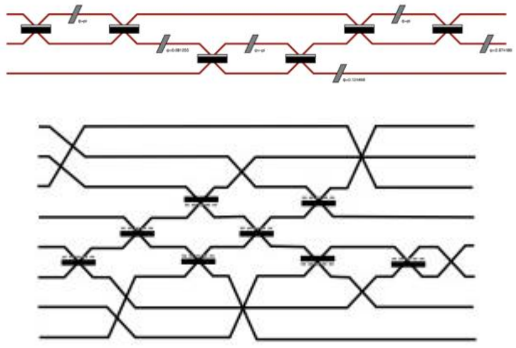
PERCEVAL

QUANDELA Cloud$_\beta$

Perceval,

Open-source programming framework for Quantum Photonics

FRONT-END INTERFACE

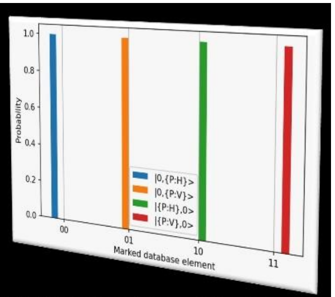


Collaborative & Open Source Tool for lectures in quantum computing

Compatible with IBM Q Qiskit

Partnership with OVHcloud

2-mode Grover's search algorithm



We implement in this notebook a 2-mode optical realization of Grover's search algorithm following *Kwiat et al. (2000). Grover's search algorithm: An optical approach. Journal of Modern Optics, 47(2–3), 257–266.* https://doi.org/10.1080/09500340008244040

Motivation

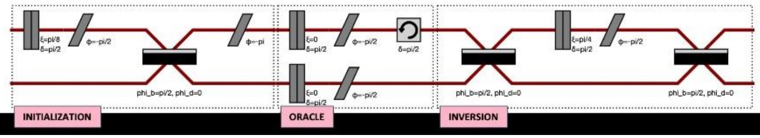
Searching for a specific item in an unstructured list of N items will classically necessitate $\mathcal{O}(N)$ function calls. Grover showed in 1996 that is possible for a quantum computer to achieve this using only $\mathcal{O}(\sqrt{N})$ iterations.

Algorithm breakdown

Suppose we are implementing Grover's algorithm with NN qubits. The algorithm's first part consists in setting each of these qubits in a quantum superposition $\frac{|0>+|1>}{\sqrt{2}}$. Then, a so-called oracle is applied on the qubits.

```python
def grover_circuit(n):
    """Returns grover circuit which selects output n, where n is 0, 1, 2 or 3."""
    grover_circuit = pcvl.Circuit(m=2, name='Grover')
    grover_circuit.add((0,1), init_circuit).add((0,1), oracle(n))\
                  .add((0,1), inversion_circuit)
    return grover_circuit

pcvl.pdisplay(grover_circuit(0), recursive=True)
```



Heurtel et al., Perceval: A Software Platform for Discrete Variable Photonic Quantum Computing, Quantum 7, 931 (2023)

7-9 Nov. 22'
Paris

(Sorbonne Université)

At the Crossroads of
Physics and Software!

LOQCathon

Powered by Quandela with a partnership of QICS (Quantum Information Center Sorbonne)


LOQCathon

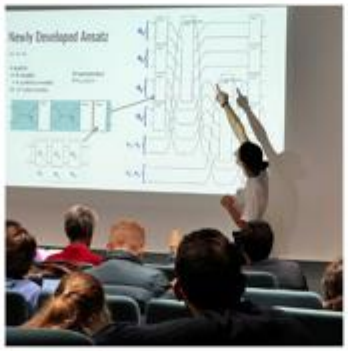





LOQCathon




LOQCathon



Newly Developed Ansatz


LOQCathon awards




LOQCathon

Collaborations:
Andrew White (Brisbane)
Fabio Sciarrino (Rome)
Roberto Osellame (Milan)
Hagai Eisenberg (Jerusalem)
Christoph Simon (Calgary)
Ian Walmsley (Oxford)
Alexia Auffèves (Singapour)
Carlos Anton (Madrid)
...

in France :
B Valiron, V. Voliotis,
S. Tanzilli, J. Claudon,
J-Ph Poizat, S Olivier,
I. Zaquine, R. Alléaume,
L Vivien, C. Ramos, ...

MARIE CURIE ACTIONS

QUANTERA

Commission européenne

îledeFrance Demain s'invente ici

ANR

NanoSaclay


P. Senellart
Credit for most of the slides !


N. Belabas


L. Lanco


O. Krebs

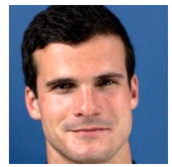

D. Kimura

C2N

Université Paris Cité

cnrs

université PARIS-SACLAY


M. Pont


A. Fyrillas


Dr. Fioretto


Dr J. Alvarez


P. Ramesh

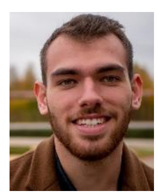

N. Coste


H. Huet


N. Margaria


I. Maillette


H. Lam


V. Guichard


A. Henry


G. Crisan


E. Medhi


M. Gundin-Martinez


A. Medeiros

A.Lemaître
I. Sagnes
@C2N

N. Maring
A. Brieussel
O. Acar M. Billard
T.-H. Au S. Boissier
P. Spetanov N. Somaschi

J. Senellart
P.-E. Emeriau
S. Mansfield
B. Boudoncle
P. Hilaire S. Wein

@QUANDELA

école normale supérieure paris—saclay | université PARIS-SACLAY

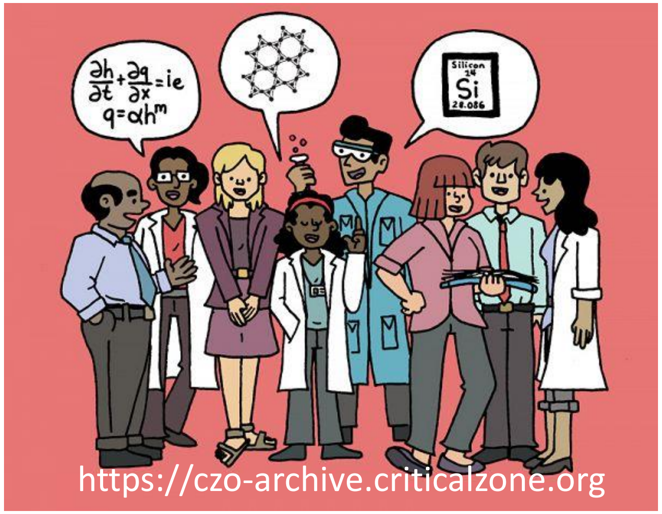
The ARTeQ year course is divided as follows:

→ **1st semester (October-January)**

Training modules
supervised research project

→ **2nd semester (February-July)**

Research internship in a public or private laboratory
+ entrepreneurship seminar



Pascale Senellart

Center for Nanoscience and Nanotechnology
CNRS– Paris Saclay University

C2N cnrs université PARIS-SACLAY

Jean Damien Pillet

Laboratoire des Solides Irradiés
Ecole Polytechnique

LSI ÉCOLE POLYTECHNIQUE IP PARIS INSTITUT POLYTECHNIQUE DE PARIS

Quantum hardware

Nadia Belabas

Center for Nanoscience and Nanotechnology
CNRS– Paris Saclay University

C2N cnrs université PARIS-SACLAY

Marino Marsi

Laboratoire de Physique des solides
Paris Saclay University

LPS ORSAY université PARIS-SACLAY

Exhibit 6 - The Current State of Progress of the Leading Hardware Technologies

		Superconductors	Ion traps	Photonics	Quantum dots	Cold atoms
% of potential users who consider technology "promising"		61%	35%	34%	26%	16%
Qubit quality[1]	*Qubit lifetime*	~1 ms	~50+ s	N/A	~1-10 s	~1 s
	Gate fidelity	~99.6%	~99.9%	~99.9%	~99%	~99%
	Gate operation time	~10-50 ns	~1-50 µs	~1 ns	~1-10 ns	~100 ns
Connectivity		Nearest neighbors	All-to-all	All-to-all[2]	Nearest neighbors	Near neighbors
Strengths		✓ Engineering maturity ✓ Scalability[3]	✓ Stability ✓ Gate fidelity ✓ Connectivity	✓ Horizontal scalability ✓ Established semiconductor tech	✓ Stability ✓ Established semiconductor tech	✓ Horizontal scalability ✓ Connectivity
Challenges		× Near absolute zero temperatures × Connectivity limitation in 2D	× Gate operation times × Horizontal scaling beyond one trap	× Noise from photon loss	× Requires cryogenics × Nascent engineering	× Gate fidelity × Gate operation time
Example players		IBM, Google	Honeywell, IonQ	PsiQuantum, Xanadu	Intel, SQC	ColdQuanta, Pasqal

Sources: Expert interviews, Science, Nature, NAE Report, Hyperion Research.

[1]Best reported performance available for all dimensions.

[2]PsiQuantum publication (March 2021).

[3]IBM and Google have announced 1M qubit roadmaps for between 2025 and 2030.

Boston Consulting Group – 2021

Platform comparisons

	Leading technologies in NISQ era[1]		Candidate technologies beyond NISQ		
Qubit type or technology	**Superconducting[2]**	**Trapped ion**	**Photonic**	**Silicon-based[3]**	**Topological[8]**
Description of qubit encoding	Two-level system of a superconducting circuit	Electron spin direction of ionized atoms in vacuum	Occupation of a waveguide pair of single photons	Nuclear or electron spin or charge of doped P atoms in Si	Majorana particles in a nanowire
Physical qubits[4,5]	IBM: 20, Rigetti: 19, Alibaba: 11, Google: 9	Lab environment: AQT[6]: 20, IonQ: 14	**6×3[9]**	**2**	target: 1 in 2018
Qubit lifetime	**~50–100 µs**	**~50 s**	**~150 µs**	**~1–10 s**	target ~100 s
Gate fidelity[7]	**~99.4%**	**~99.9%**	**~98%**	**~90%**	target ~99.9999%
Gate operation time	**~10–50 ns**	**~3-50 µs**	**~1 ns**	**~1–10 ns**	–
Connectivity	Nearest neighbors	All-to-all	To be demonstrated	Nearest neighbor	–
Scalability	No major road-blocks near-term	Scaling beyond one trap (>50 qb)	Single photon sources and detection	Novel technology potentially high scalability	?
Maturity or technology readiness level	TRL[10] 5	TRL 4	TRL 3	TRL 3	TRL 1
Key properties	Cryogenic operation Fast gating Silicon technology	Improves with cryogenic temperatures Long qubit lifetime Vacuum operation	Room temperature Fast gating Modular design	Cryogenic operation Fast gating Atomic-scale size	Estimated: Long lifetime High fidelities

Boston Consulting Group – Nov 2018

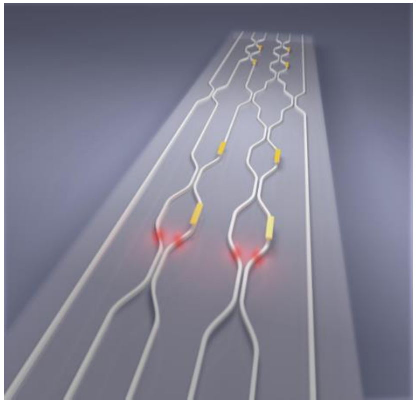
Applications of a universal quantum computer

INDUSTRIES	SELECTION OF USE-CASES	ENTERPRISES (EXAMPLES)
High-tech	• Machine learning and artificial intelligence, such as neural networks • Search • Bidding strategies for advertisements • Cybersecurity • Online and product marketing • Software verification and validation	IBM, Telstra, Alibaba, Baidu, Google, Samsung, Microsoft
Industrial goods	• Logistics: scheduling, planning, product distribution, routing • Automotive: traffic simulation, e-charging station and parking search, autonomous driving • Semiconductors: manufacturing, such as chip layout optimization • Aerospace: R&D and manufacturing, such as fault-analysis, stronger polymers for airplanes • Material science: effective catalytic converters for cars, battery cell research, more-efficient materials for solar cells, and property engineering uses such as OLEDS	Airbus, BMW, NASA, Volkswagen, Northrop Grumman, Lockheed Martin, Daimler, Honeywell, Raytheon, Bosch
Chemistry and Pharma	• Catalyst and enzyme design, such as nitrogenase • Pharmaceuticals R&D, such as faster drug discovery • Bioinformatics, such as genomics • Patient diagnostics for health care, such as improved diagnostic capability for MRI	BASF, JSR, Biogen, DuPont, Dow Chemical, Amgen
Finance	• Trading strategies • Portfolio optimization • Asset pricing • Risk analysis • Fraud detection • Market simulation	J.P. Morgan, Barclays, Commonwealth Bank, Goldman Sachs
Energy	• Network design • Energy distribution • Oil well optimization	Dubai Electricity & Water Authority, BP

Credit: The Next Decade in Quantum Computing and How to Play - Boston Consulting Group

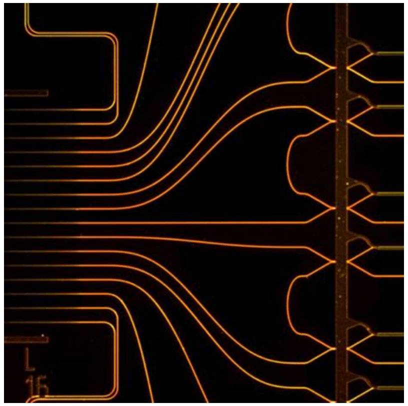
Optical quantum computing companies

PsiQuantum - USA - 2016



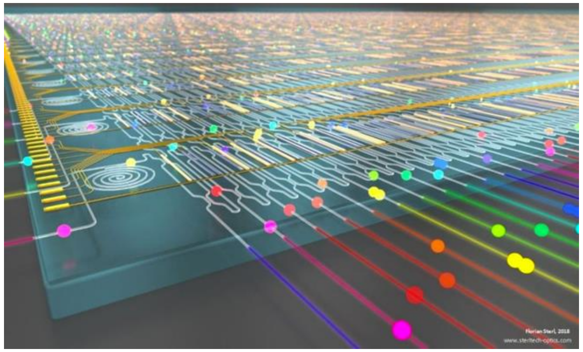
Universal CMOS optical quantum computer

Xanadu - Canada- 2018



Quantum computing powered by light

QuiX- Netherland- 2019



SiN4 based quantum computing

ORCA – UK - 2019

ORCA Computing