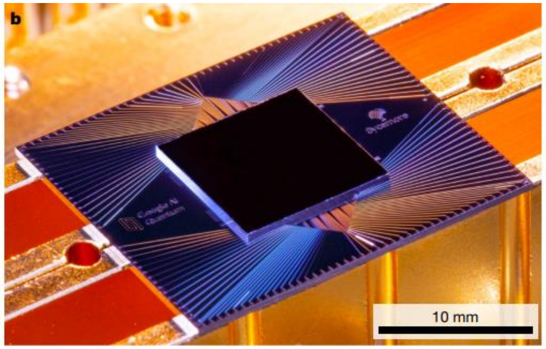
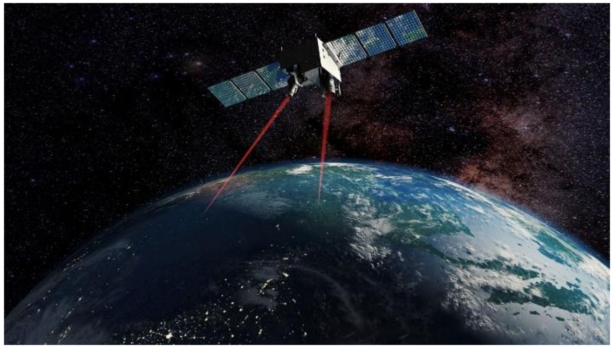
Quantum Technologies A.D. 2020

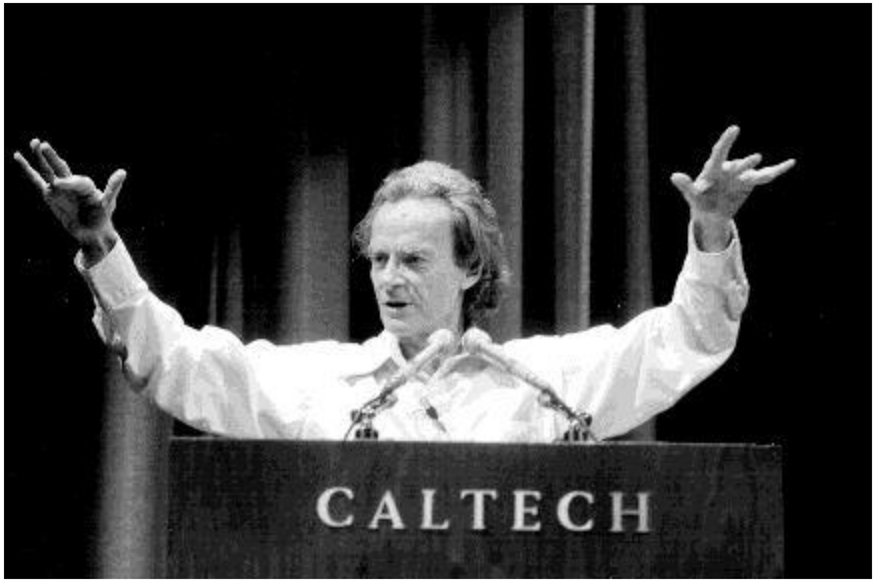
Expectations vs. Reality





Rafał Demkowicz-Dobrzański, Wydział Fizyki UW

Visions



There is plenty of room at the bottom […] nothing that I can see in the physical laws . . . says the computer elements cannot be made enormously smaller than they are now.

Richard Feynman,1959

Now, we can, in principle make a computing device in which the numbers are represented by a row of atoms with each atom in either of the two states.[…] The ones move around, the zeros move around . . Finally, along a particular bunch of atoms, ones and zeros . . . occur that represent the answer. Nothing could be made smaller . . . Nothing could be more elegant.

Richard Feynman, 1983

More visions... and money


Quantum Manifesto
A New Era of Technology
May 2016

EU Quantum Flagship programme (2018): **€ 1b** over 10 years

Long term goals (>10 years)
- Quantum internet connecting major cities in Europe
- A universal quantum computer
- On-chip quantum sensor devices that can integrate within mobile phones

UK NATIONAL
QUANTUM
TECHNOLOGIES
PROGRAMME

UK Quantum technologies programme (2013): **£ 270 mln**

US National Quantum Initiative Act (2018) 2018: **$1.2b**

Chineese National Laboratory for Quantum Information Sciences (2020) **$10b**

Comericial companies involved:
Google, IBM, Intel, Toshiba, NTT, Huawei…

Three pillars of quantum technologies

Quantum computing

Quantum communication

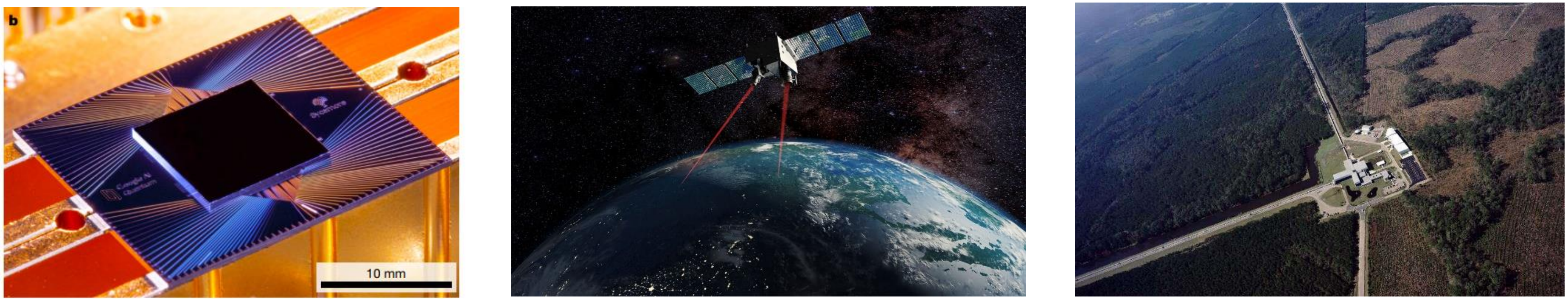
Quantum metrology

Three pillars of quantum technologies

Quantum computing

Quantum communication

Quantum metrology



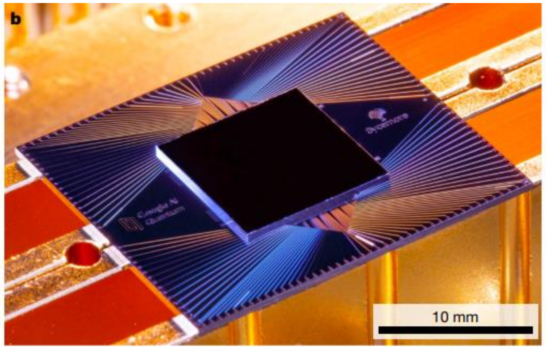
A.D. 2020 achievements

Three pillars of quantum technologies

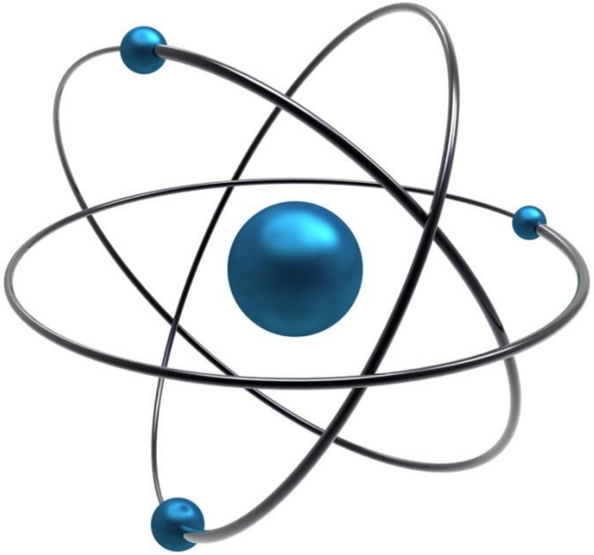
Quantum computing

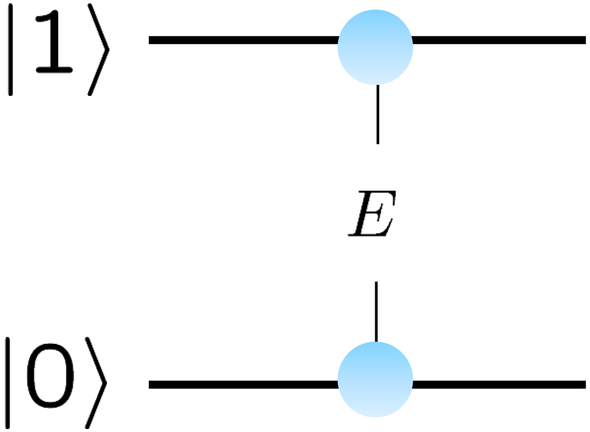
Quantum communication

Quantum metrology



Qubit



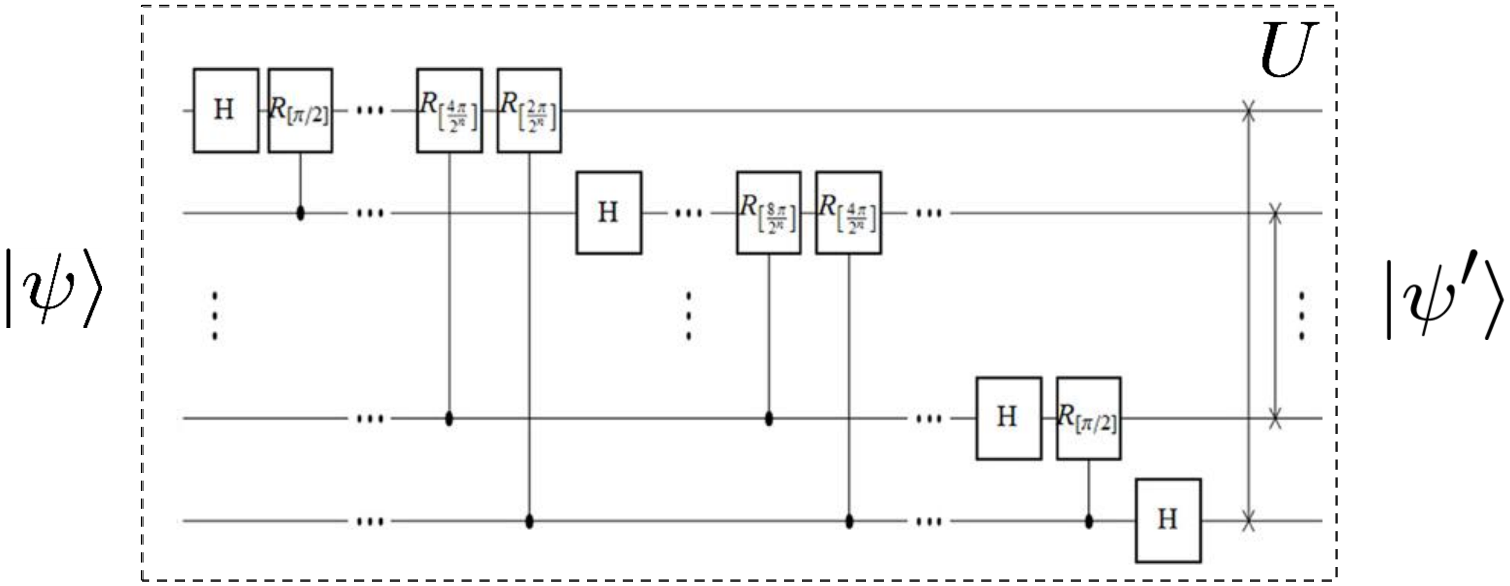


$$|\psi\rangle = a|0\rangle + b|1\rangle$$

↑

quantum superposition

Quantum parallelism



N qubits prepared as a superposition of 2^N numbers

$$|\psi\rangle = |00\ldots0\rangle + |00\ldots1\rangle + \ldots + |11\ldots1\rangle$$

In a single run we process present in the superposition

$$|\psi'\rangle = U|00\ldots0\rangle + U|00\ldots1\rangle + \ldots + U|11\ldots1\rangle$$

How to read out the result?
We can only distniguish orthogonal vectors!

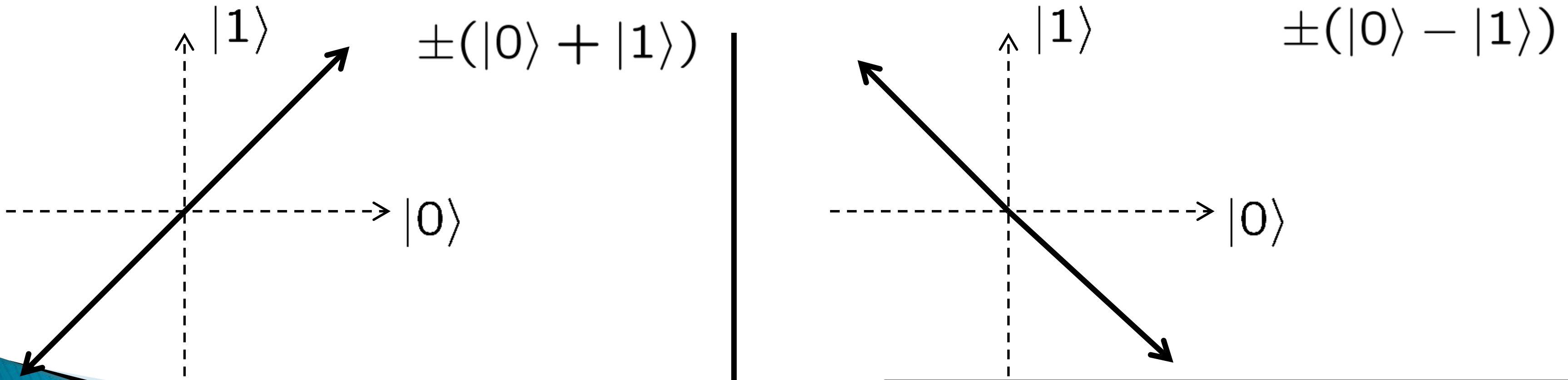
Deutsch algorithm (1985)

$f : \{0, 1\} \rightarrow \{0, 1\}$ - single bit function

$f(0) = f(1)?$ | $f(0) \neq f(1)?$

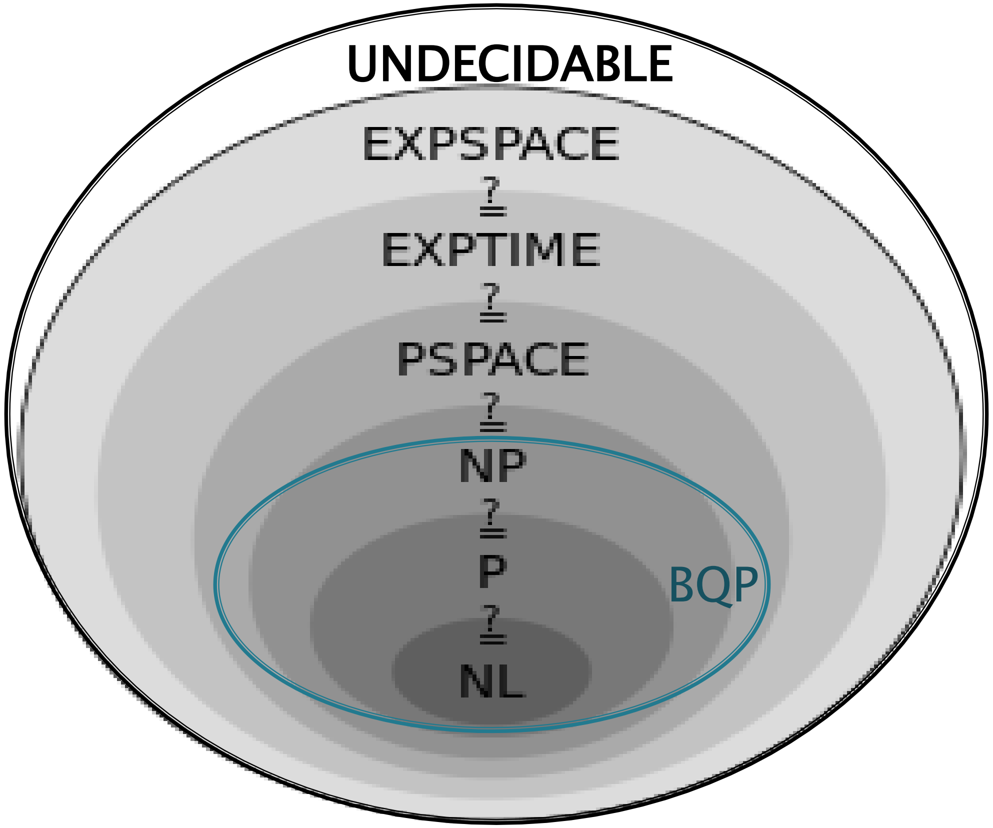
classically we need to compute f two times

$$U_f|x\rangle = (-1)^{f(x)}|x\rangle \qquad U_f(|0\rangle + |1\rangle) = (-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle$$



It is enough to ask the quantum oracle only once!

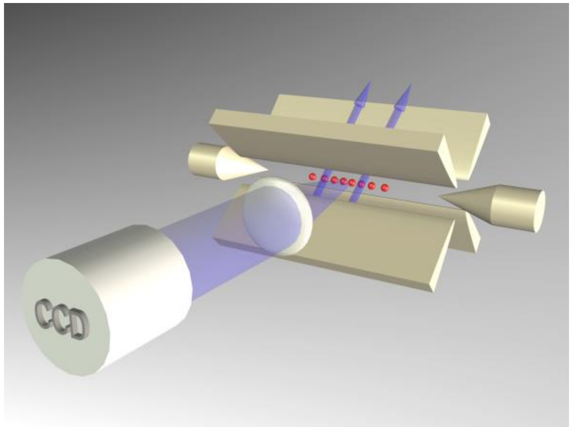
Computation complexity theory including quantum algorithms



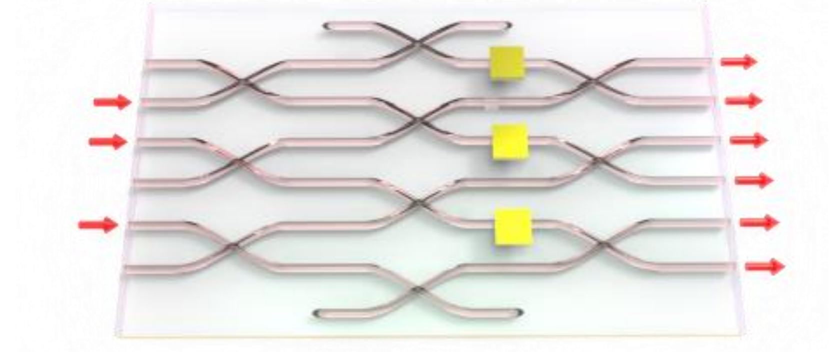
- Deutsch algorithm (1985)
- Shor’s algorithm (1994)
- Grover’s algorithm (1996)
- Graph connectivity (2004)
- Sparse matrix inversion (2007)
- Customer recommendation systems (2016)
- …
  quantumalgorithmzoo.org

BQP – bounded error quantum polynomial time

On the way to build a quantm computer

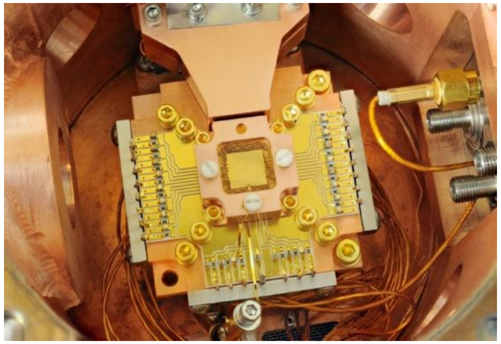


Ion traps ~15 qubits



single photons in optical integrated circuits ~12 photons

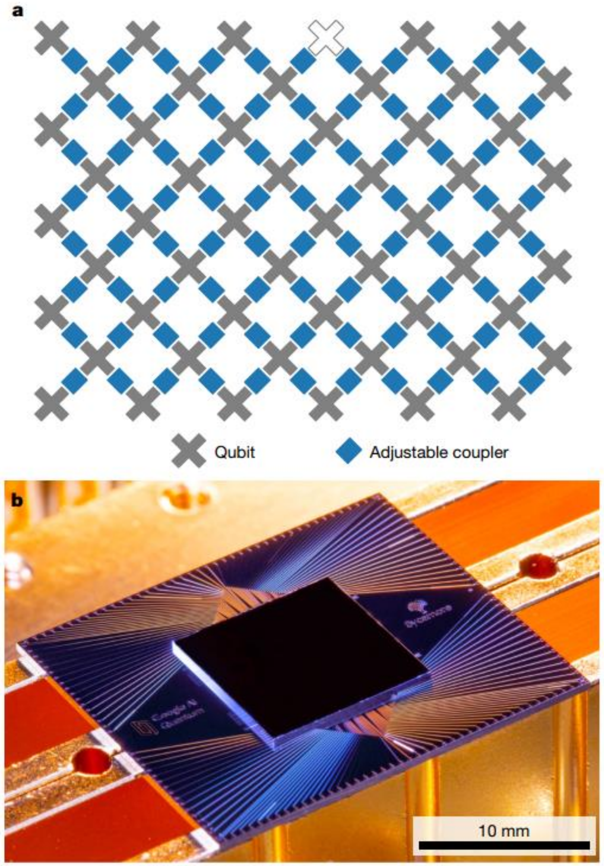
Superconducting qubits



50 qubit quantum computing device (IBM, 2017)

~2000 qubit quantum annealing device (adiabatic computing) (DWAVE, 2017)

Google quantum supremacy demonstration

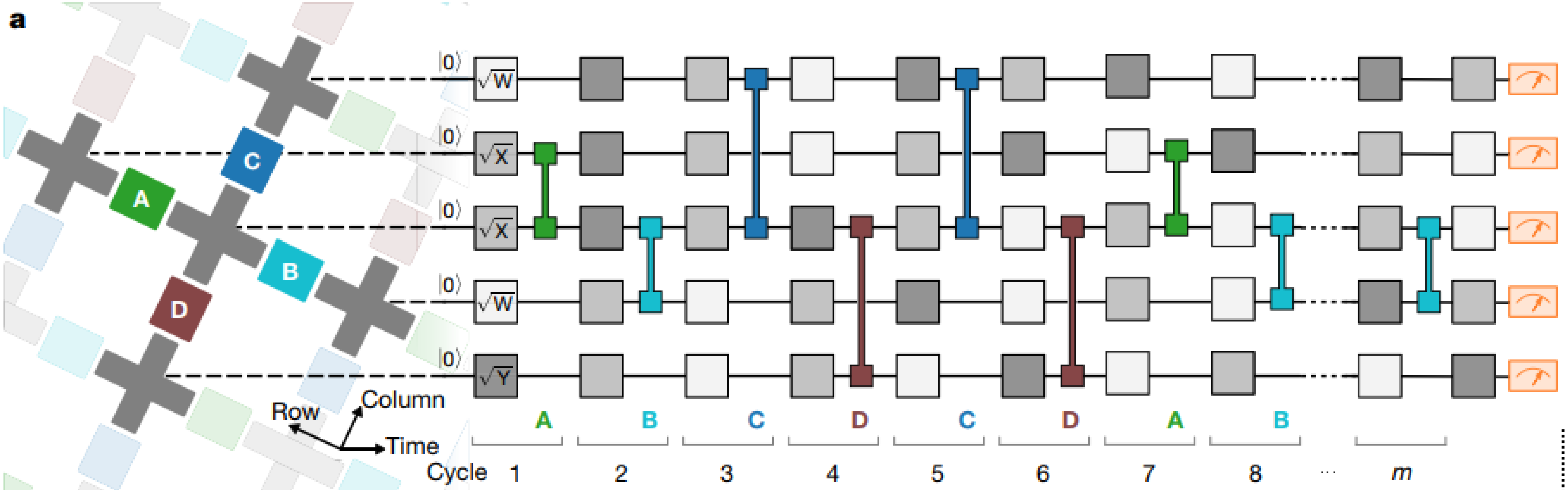


Sycamore (53 qubit quantum device)

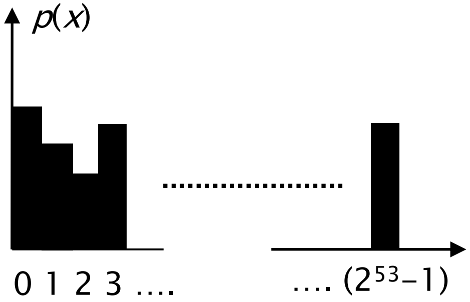
[…] Here we report the use of a processor with programmable superconducting qubits to create quantum states on 53 qubits, corresponding to a computational state-space of dimension 2^{53} (about 10^{16}). Measurements from repeated experiments sample the resulting probability distribution, which we verify using classical simulations. Our Sycamore processor takes about 200 seconds to sample one instance of a quantum circuit a million times—our benchmarks currently indicate that the equivalent task for a state-of-the-art classical supercomputer would take approximately 10,000 years […]

Nature **574**, 505-510 (2019)

Random quantum circuit is difficult to simulate classically



$n = 53$



Goal: sample from this probability distribution

Nature **574**, 505–510 (2019)

IBM rebuttal of Google's claim…

$2^{53} \approx 10 \text{ PB} < 250 \text{ PB}$

We argue that an ideal simulation of the same task can be performed on a classical system in 2.5 days and with far greater fidelity.

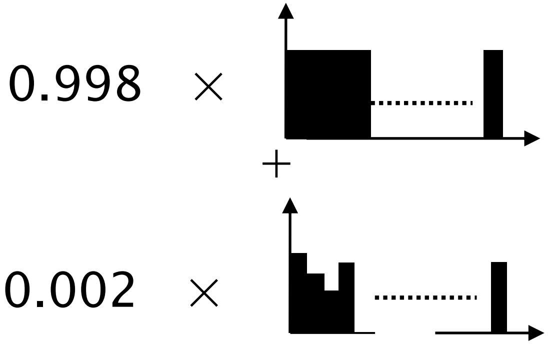
IBM researchers Edwin Pednault, John Gunnels, and Jay Gambetta

Noisy Intermediate Scale Quantum Computing (NISQ)

Errors too large (10^{-2} –10^{-3}) to implement effectively quantum error correction codes.

Find any kind of task (useful or not useful) in which quantum computing device can outperfom classial supercomputers despite presence of noise

Because of noise, what Google's device actually samples from is:



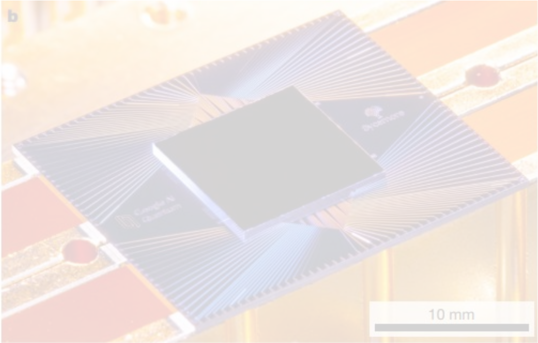
If we want more, we need to reach the fault tollerant regime (errors on the order of 10^{-4}) and implement quantum error-correction codes.

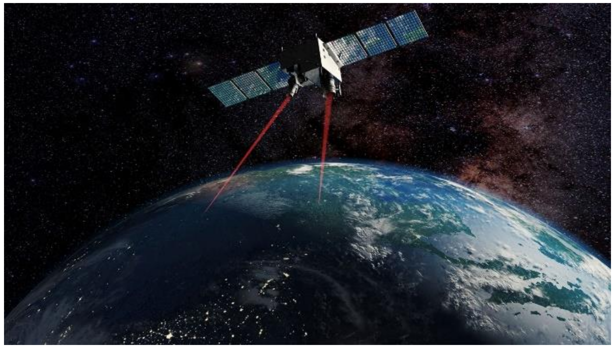
Three pillars of quantum technologies

Quantum computing

Quantum communication

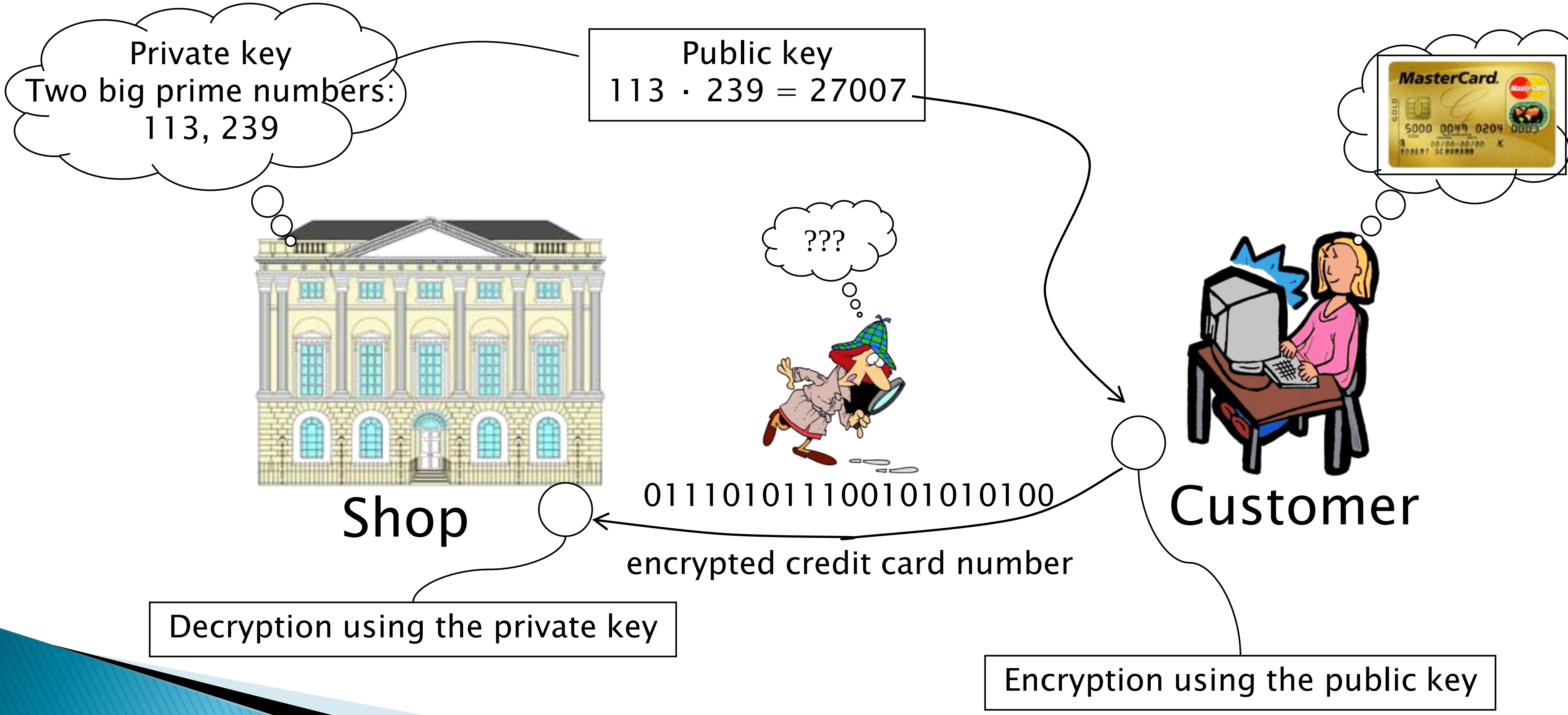
Quantum metrology





https:// is believed to be secure because we believe factoring is hard

RSA protocol:



Private key
Two big prime numbers:
113, 239

Public key
113 · 239 = 27007

Shop

Customer

011101011100101010100

encrypted credit card number

Decryption using the private key

Encryption using the public key

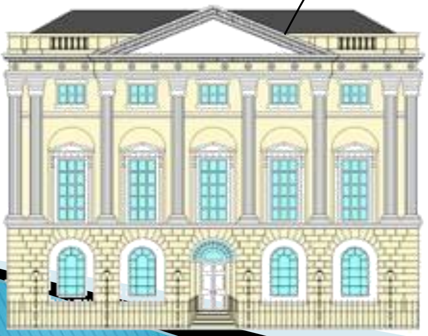
Perfectly secure cryptographic method: One–time pad

If the two parties share a random secret key of the lenght equal to the lenght of the message

0+0=0
0+1=1
1+0=1
1+1=0

Information: 10101010101010
+
Key: 11101001011001
Encrypted Information: 01000011110011

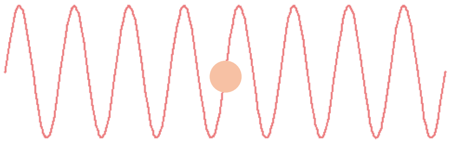
Information: 10101010101010
Key: 11101001011001
+
Encrypted information: 01000011110011



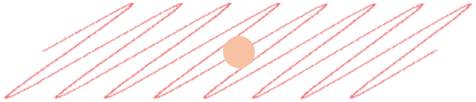
But how to distribute the key?

Secure quantum key distribution: BB84 protocol (1984)

Single photon polarization state as a qubit



$$|\updownarrow\rangle = |0\rangle$$

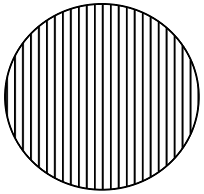


$$|\leftrightarrow\rangle = |1\rangle$$

Arbitrary linear polarization:

$$|\alpha\rangle = \cos(\alpha)|\updownarrow\rangle + \sin(\alpha)|\leftrightarrow\rangle$$

Measurement:

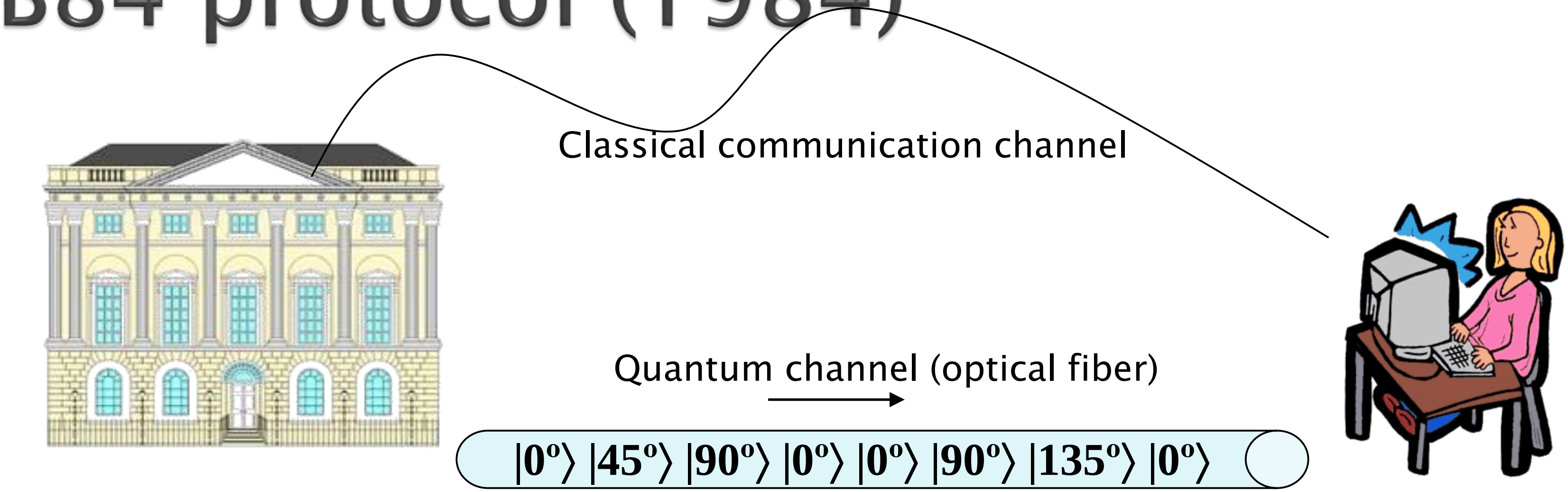


polarizer

$$\{|\updownarrow\rangle, |\leftrightarrow\rangle\}$$

measurement basis

Secure quantum key distribution: BB84 protocol (1984)



Classical communication channel

Quantum channel (optical fiber)

$|0^\circ\rangle$ $|45^\circ\rangle$ $|90^\circ\rangle$ $|0^\circ\rangle$ $|0^\circ\rangle$ $|90^\circ\rangle$ $|135^\circ\rangle$ $|0^\circ\rangle$

The sender sends a state

basis 1:	$\|0^\circ\rangle$	$\|90^\circ\rangle$
basis 2:	$\|45^\circ\rangle$	$\|135^\circ\rangle$
bit	0	1

The receiver chooses a measurement

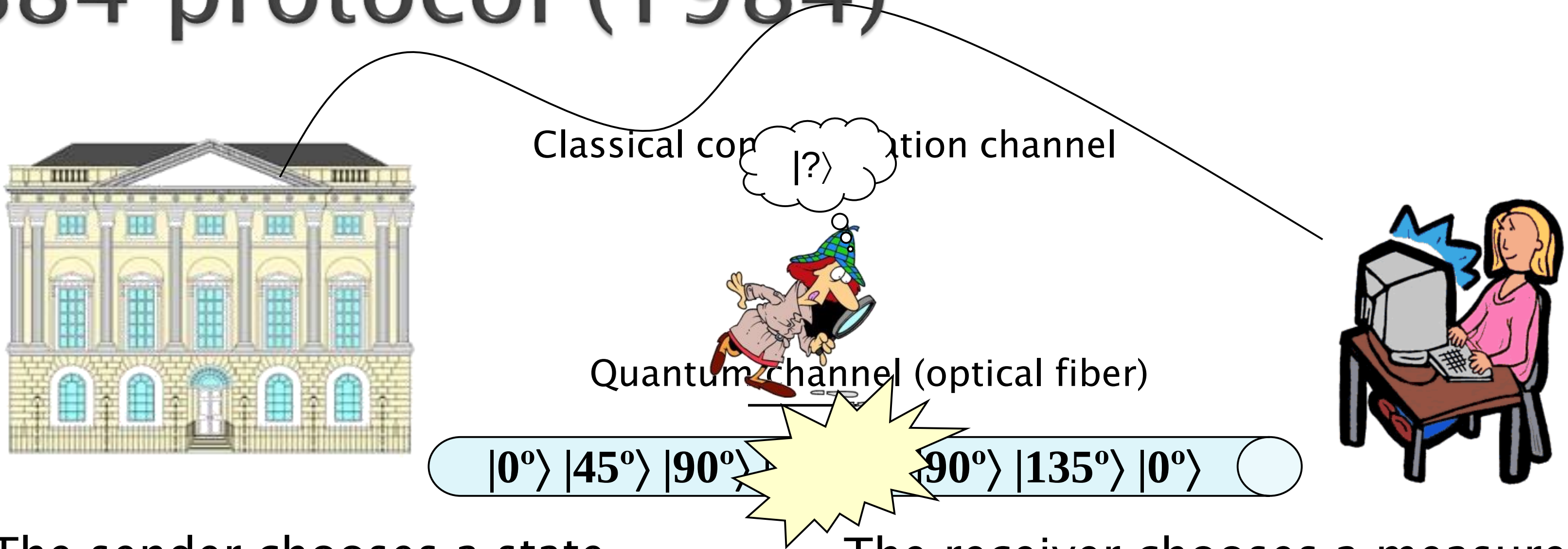
▥ basis 1

▨ basis 2

After the transmission they throw away bits obtained from measurements in incompatible basis

Nonorthogonal state cannot be distinguished perfectly.

Secure quantum key distribution: BB84 protocol (1984)



The sender chooses a state

basis 1:	$|0^\circ\rangle$	$|90^\circ\rangle$
basis 2:	$|45^\circ\rangle$	$|135^\circ\rangle$
bit	0	1

The receiver chooses a measurement

▥ basis 1

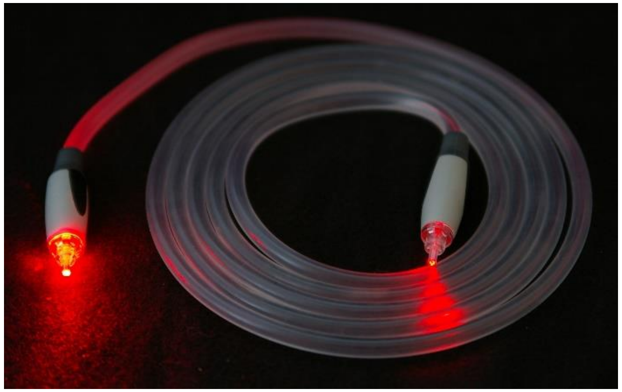
▨ basis 2

After the transmission they throw away bits obtained from measurements in incompatible basis

The more information eavesdropper obtains the bigger disturbance he introduces

The main challenge: photon loss

Optical fibers

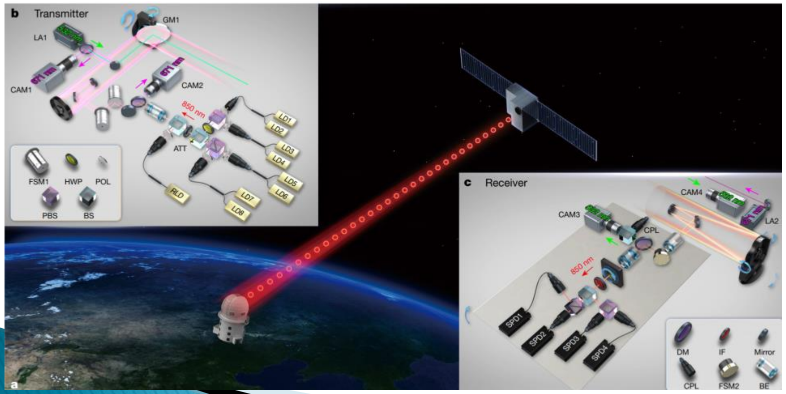


Loss ~0.2 dB per km @1500nm

Probability that a single photon survives a 400km transmission: 10^{-8}

Quantum key distribution record:
6 bit/s of secure key at 425km
Phys. Rev. Lett. 121, 190502 (2018)

Free space

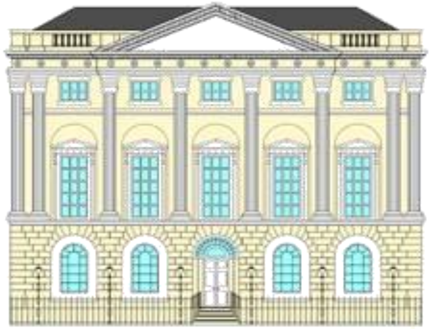


Atmospheric loss: 5 dB (~10km of atmosphere) + diffraction loss

Micius Satellite: 1 kbit/s over 1200km
Nature 549, 43 (2017)

Distributing a key between Austria and China (7600km) via trusted Satelite
Phys. Rev. Lett. 120, 030501 (2018)

Entanglement based protocols



$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|\updownarrow\rangle \otimes |\leftrightarrow\rangle + |\leftrightarrow\rangle \otimes |\updownarrow\rangle\right)$$

E91 protocol (A. Ekert, 1991)

Both parties perform measurements choosing one of two measurement basis, obtaining the key and checking the strength of correlations.

Security related with the fact that local hidden variable theories cannot reproduce quantum correlations (Bell inequalities)

Micius Satellite: entanglement distribution between ground stattions separated by over 1200 km (~1pair/s)

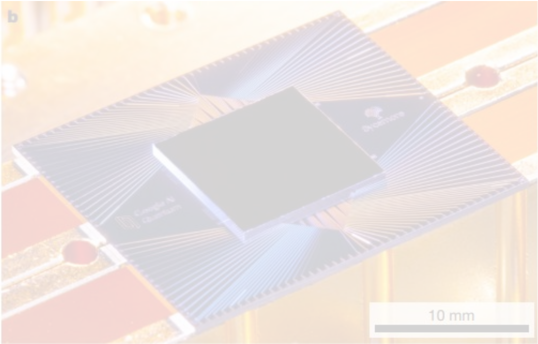
Science 356, 1140 (2017)

Three pillars of quantum technologies

Quantum computing

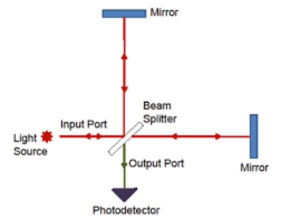
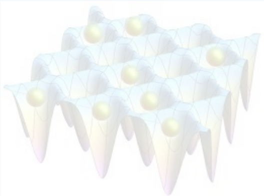
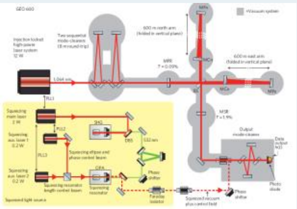
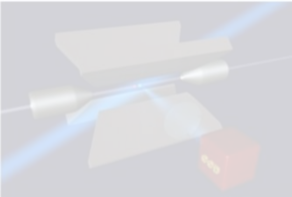
Quantum communication

Quantum metrology



Quantum Metrology

manipiulate individual quantum systems to make the most of quantum coherence (and entanglement) in order to boost measurement precision

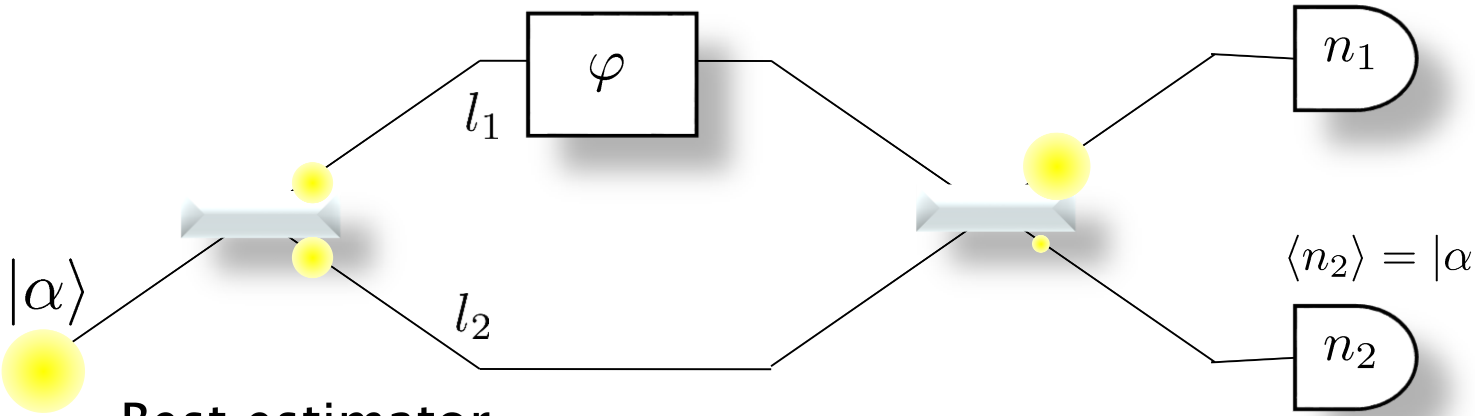
	Optical interfereometry	Atomic interferometry	Solid state (e.g. NV centers)
Coherence	 „classical" light	 uncorrelated/single atoms	 electron spin only
Entanglement	 squeezed light	 entangled atoms	 electron spin entangled with nuclear spins
Decoherence	photon loss	LO fluctuations, atom dephasing, loss	spin dephasing

„Classical" interferometry

$$\varphi = 2\pi(l_1 - l_2)/\lambda$$

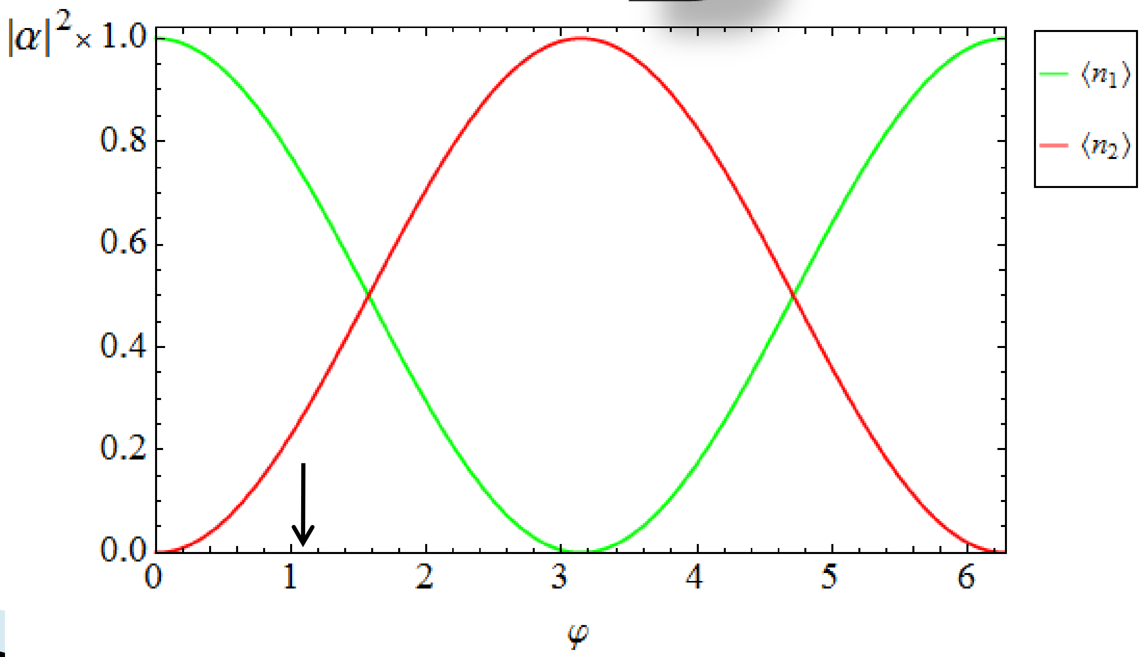
$$\langle n_1 \rangle = |\alpha|^2 (1 + \cos\varphi)/2$$

$$\langle n_2 \rangle = |\alpha|^2 (1 - \cos\varphi)/2$$

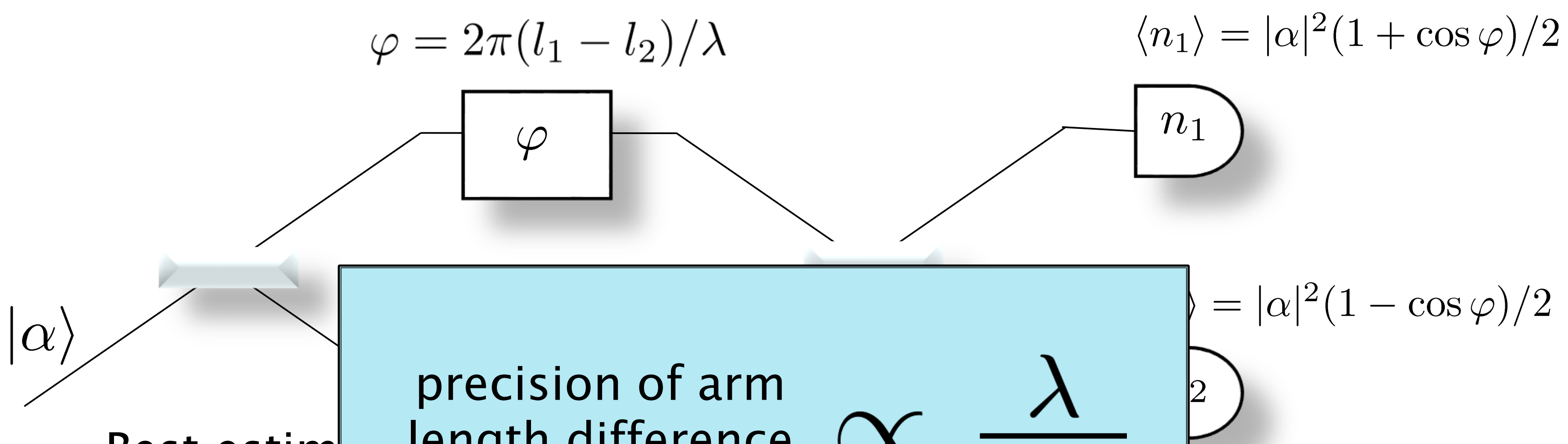


Best estimator

$$\varphi(n_1, n_2) = \arccos\left(\frac{n_1 - n_2}{|\alpha|^2}\right)$$



„Classical" interferometry



precision of arm length difference estimation $\propto \dfrac{\lambda}{\sqrt{\bar{n}}}$

Best estim

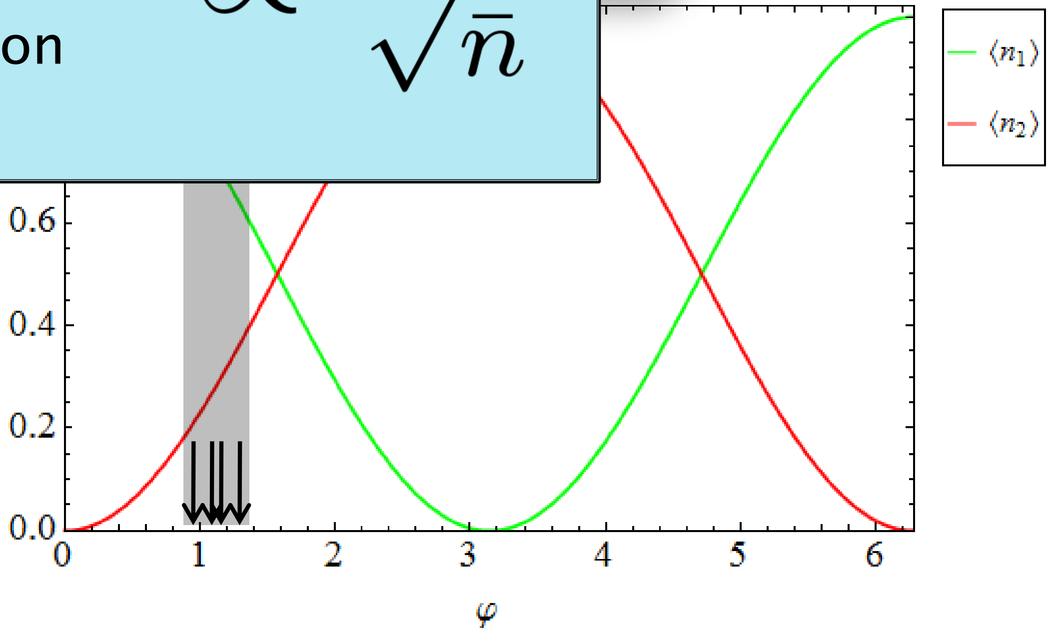
$\varphi(n_1, n_2) = \mathrm{arcc}$

Poissonian statsitics

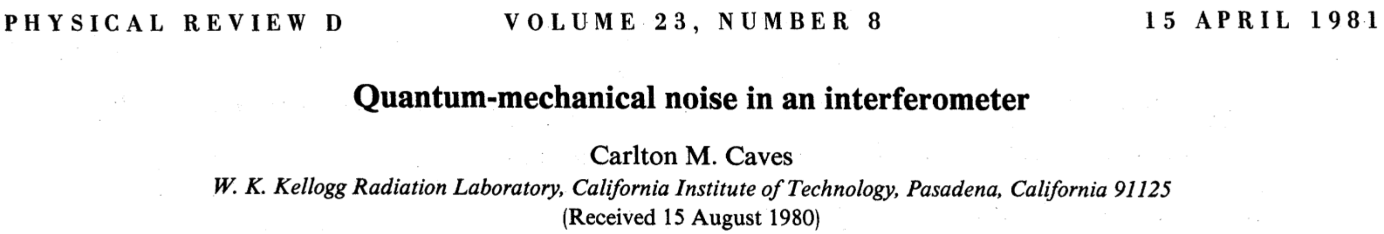
$$n_i = \langle n_i \rangle \pm \sqrt{\langle n_i \rangle}$$

$$\Delta\varphi \propto \frac{1}{|\alpha|} = \frac{1}{\sqrt{\bar{n}}}$$

Shot noise scaling



Squeezed states

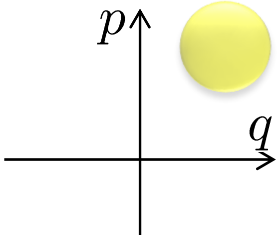


PHYSICAL REVIEW D VOLUME 23, NUMBER 8 15 APRIL 1981

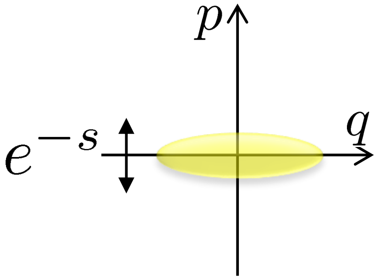
Quantum-mechanical noise in an interferometer

Carlton M. Caves
W. K. Kellogg Radiation Laboratory, California Institute of Technology, Pasadena, California 91125

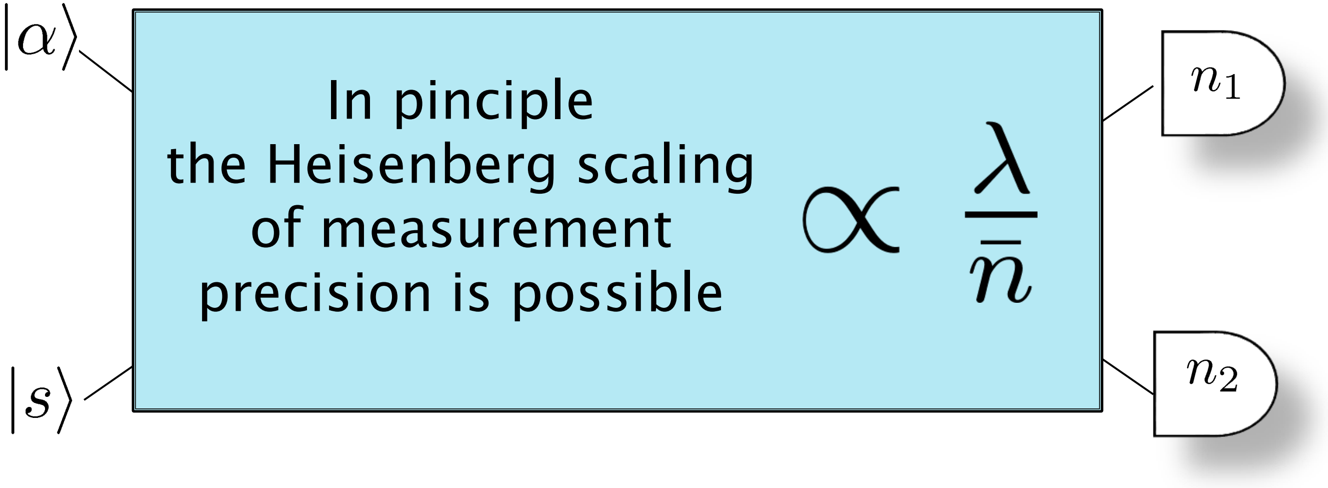
(Received 15 August 1980)



coherent state



squeezed vacuum

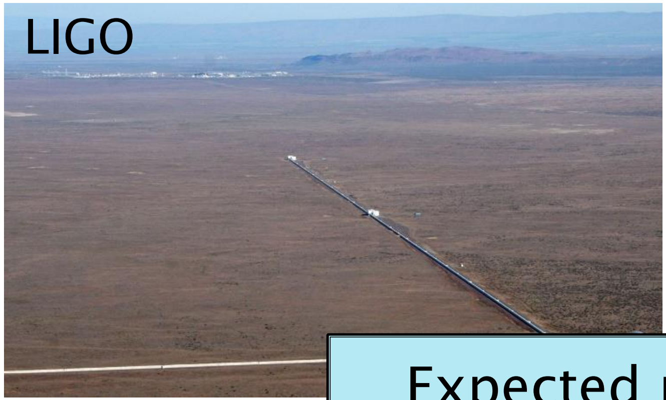


In pinciple
the Heisenberg scaling
of measurement
precision is possible $\propto \dfrac{\lambda}{\bar{n}}$

Better sensitivity thanks to sub-Poissonian fluctuations of $n_1 - n_2$!

Squeezing can be understood as a form of entanglement between photons

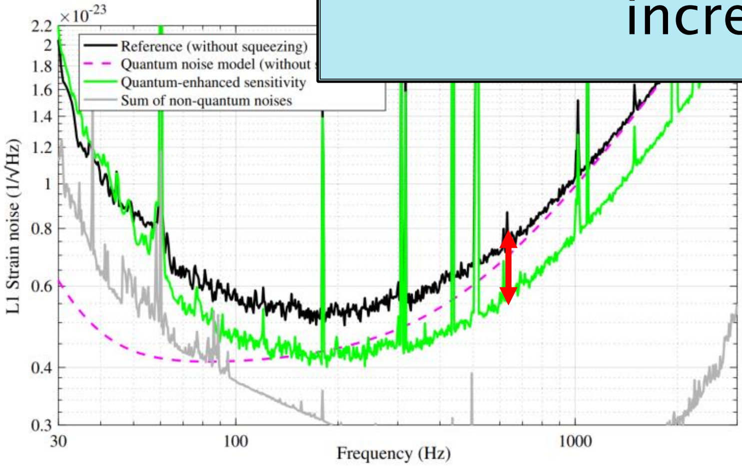
Squeezed light enhanced gravitational wave detectors

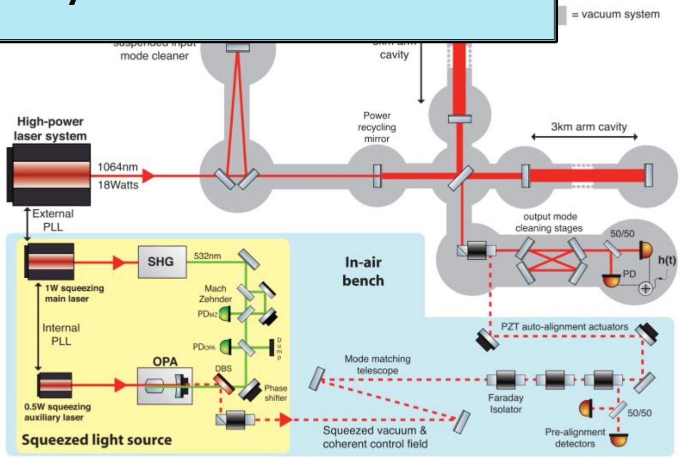


Phys. Rev. Lett. 12

19)

Expected number of binary neutron star merger detection events increased by 50%!





35% reduction of noise thanks to squeezing – equivalent of increasing the power by 85%!

~100 `quantum' photons contribute the same improvement as $10^{20}$ `classical' photons

Three pillars of quantum technologies

Quantum computing

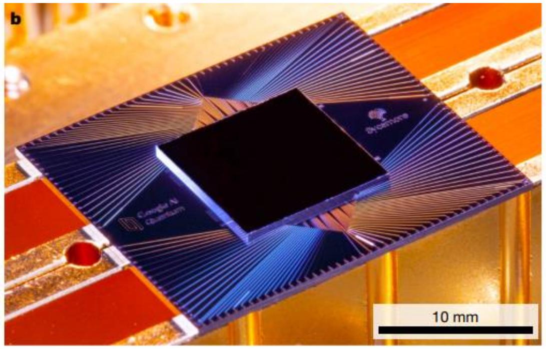
- reach noise fault-tollerant threshold
- implement quantum error-correction

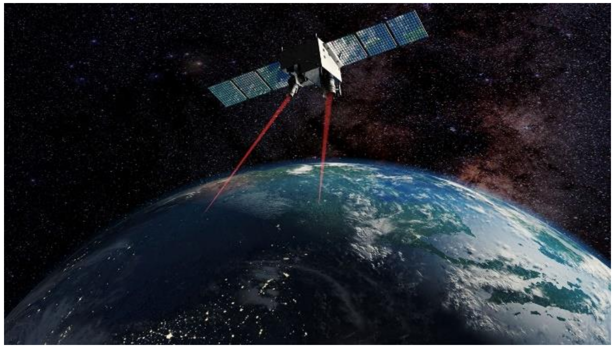
Quantum communication

- reduce loss
- develop quantum repeaters

Quantum metrology

- reduce noise
- adapt error-correction protocols from quantum computing





A.D. 2020 achievements and challenges