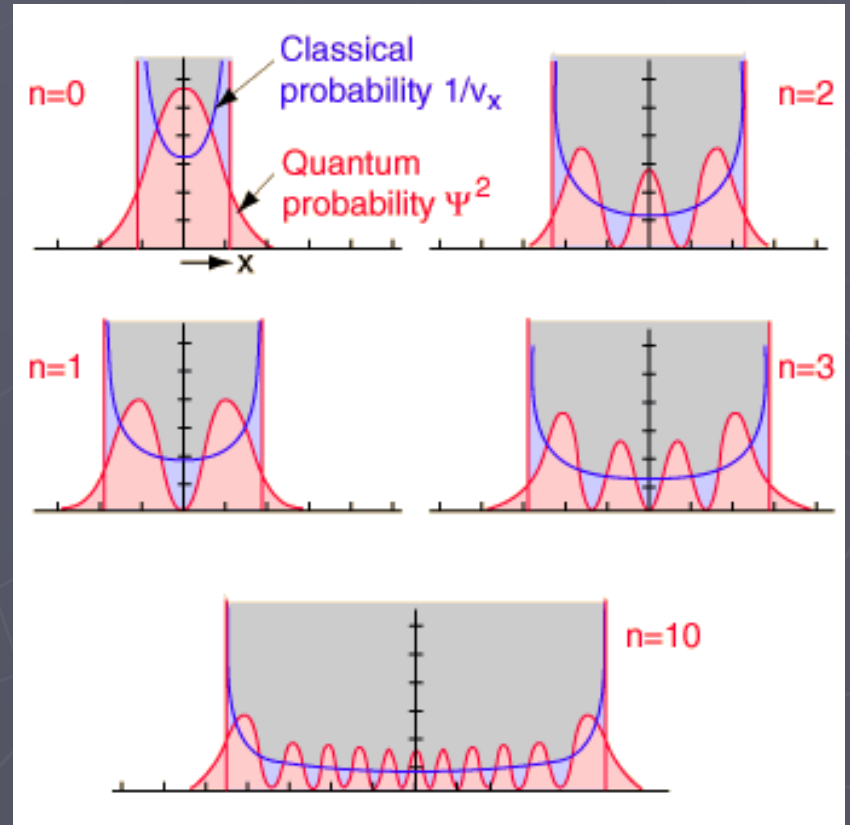
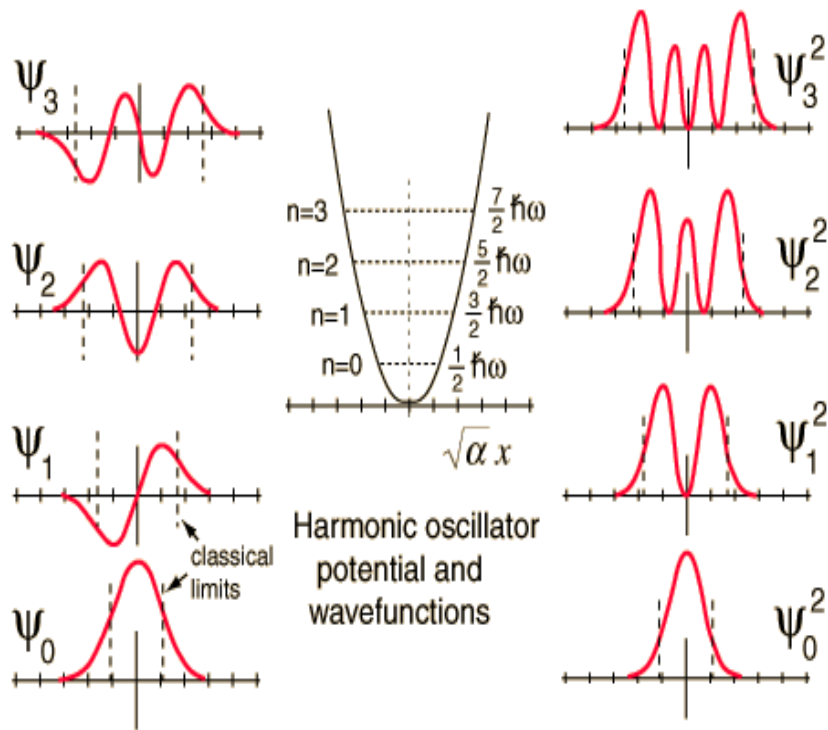


Physics is becoming too  
difficult for physicists.

— David Hilbert  
(mathematician)



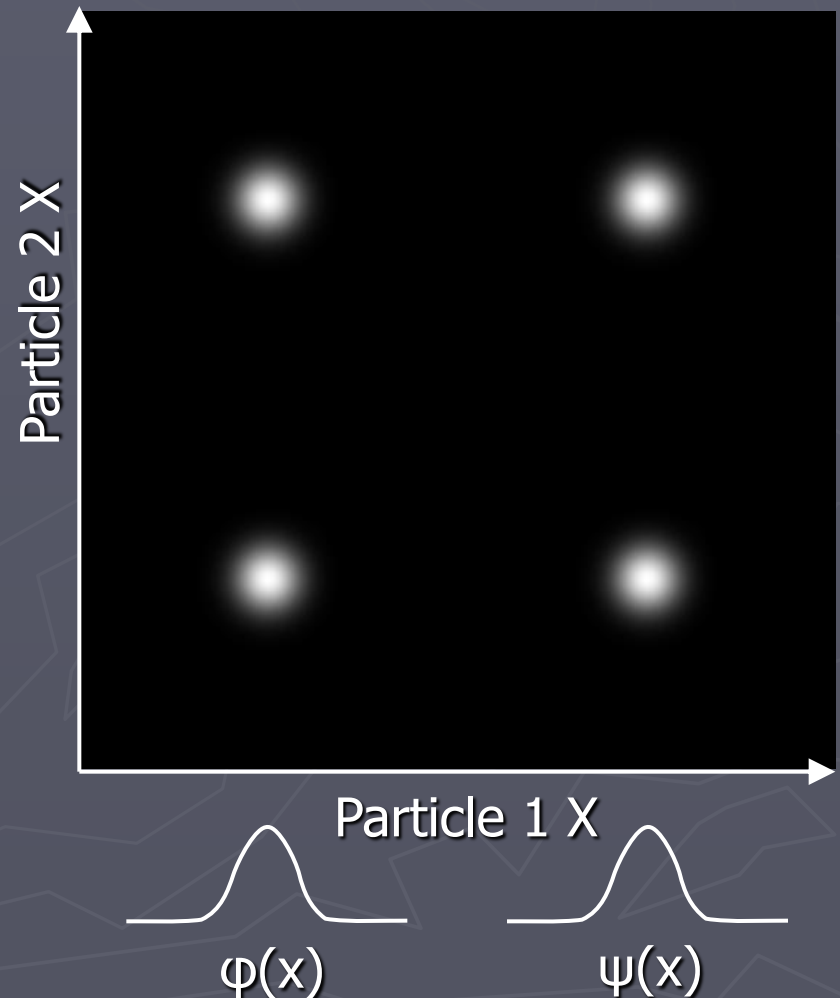
# Simple Harmonic Oscillator



Credit: R. Nave (HyperPhysics)

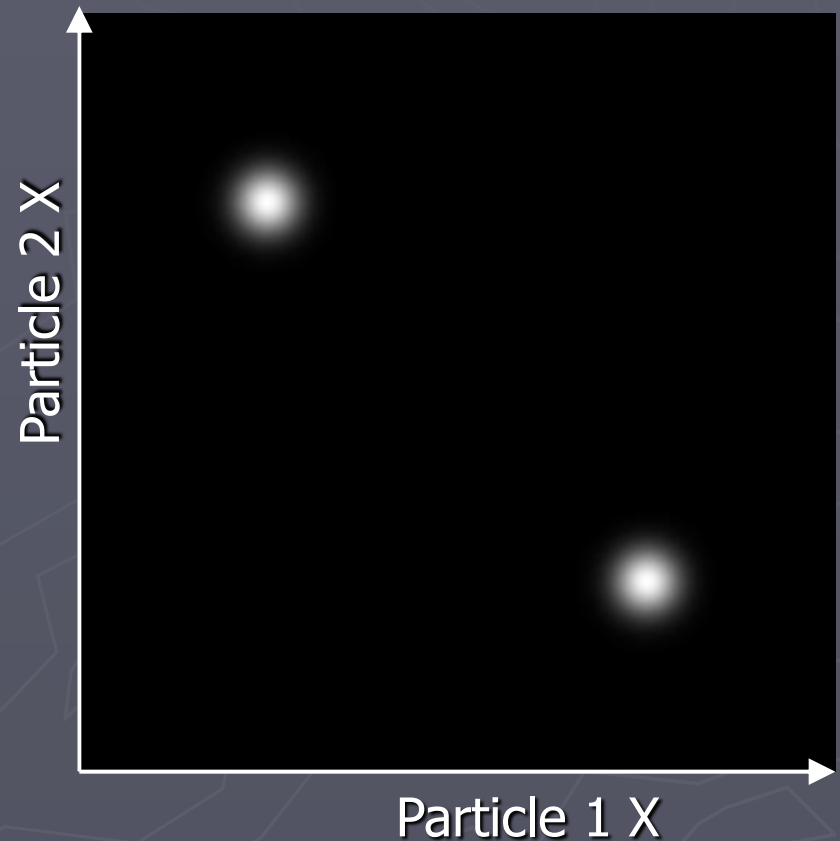
# 2-Particle wave functions

- ▶ 2 Particles, each moving in 1 D, i.e. along the X axis
- ▶ Then **configuration space** is 2 dimensional:  $x_1, x_2$ .
- ▶ Here each particle is in a superposition of two wave packets, say  $\psi(x)$  and  $\phi(x)$ .
  - e.g. they may have just gone through a double slit.
- ▶ Position of each particle is independent of the other, so we can factorise wave function:
  - $\Psi(x_1, x_2) = [ \psi(x_1) + \phi(x_1) ] [ \psi(x_2) + \phi(x_2) ]$
  - or  $|\Psi\rangle = ( |\psi\rangle + |\phi\rangle ) \otimes ( |\psi\rangle + |\phi\rangle )$



# 2-Particle wave functions

- ▶ Now particle positions are **correlated**.
- ▶ Particles are still in a superposition of two possible positions...
- ▶ ...but position of each particle depends on the other:
  - if particle 1 went through right slit, particle 2 went through left, and vice versa.
- ▶ Wave function is composite:
  - $\Psi(x_1, x_2) =$   
 $\psi(x_1) \phi(x_2) + \phi(x_1) \psi(x_2)$
  - or  $|\Psi\rangle = |\psi\rangle \otimes |\phi\rangle + |\phi\rangle \otimes |\psi\rangle$
  - NB: *two products!*



# Applications of Entanglement

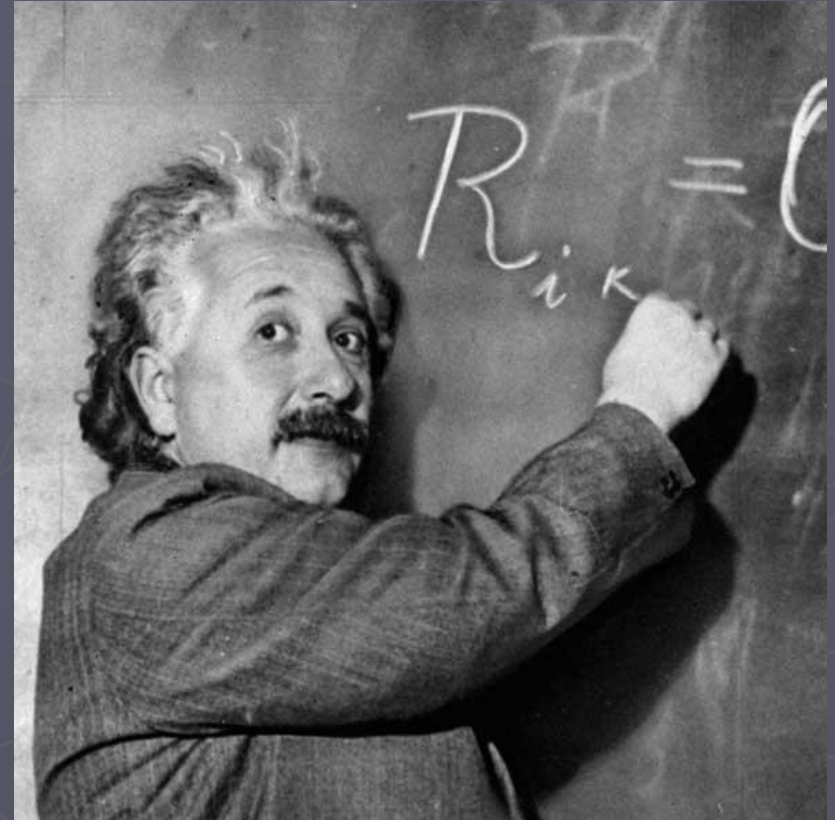
- ▶ Tests of non-locality (Bell inequalities etc)
- ▶ Quantum cryptography
- ▶ Quantum computing
- ▶ Quantum teleportation
- ▶ Interface between quantum and classical worlds





# Einstein, Podolsky & Rosen (1935)

- ▶ “Is Quantum Mechanical Description of reality complete?”
- ▶ Create entangled pair of particles with correlated position and momentum:
  - Measure momentum of particle A, tells you automatically momentum of particle B
  - Measure position of particle B, tells you position of A
- ▶ Let particles separate and measure mom of A and pos of B at the same time:
  - Apparently give  $x$  and  $p$  of both particles (just before measurement)
  - Breaks uncertainty principle?
- ▶ No practical use as measurements disrupt  $p$  of A and  $x$  of B!



# Bell Inequalities

- ▶ Measurements at non-orthogonal angles for local theory must satisfy certain inequalities in their probabilities of results, which Bohm states violate.
- ▶ Experiments (1980s) confirm QM prediction, i.e. violation of Bell inequalities



# Qubit

- ▶ Classical computer: store data as binary digits (bits) 0 or 1.
- ▶ Quantum computer: store data in 2-level systems (Qubits) with eigenstates  $|0\rangle$  &  $|1\rangle$  (or  $|g\rangle$  &  $|e\rangle$  for ground and excited)
  - e.g. spin up & spin down; ground & 1<sup>st</sup> excited state of oscillator, etc.
- ▶ Quantum logic gates change state of qubit eigenstates.
  - E.g. quantum not gate:

$$\begin{array}{l} |\text{input}\rangle |\text{output}\rangle \\ |0\rangle |0\rangle \rightarrow |0\rangle |1\rangle \\ |1\rangle |0\rangle \rightarrow |1\rangle |0\rangle \end{array}$$

- ▶ If qubit is in superposition, output is entangled:

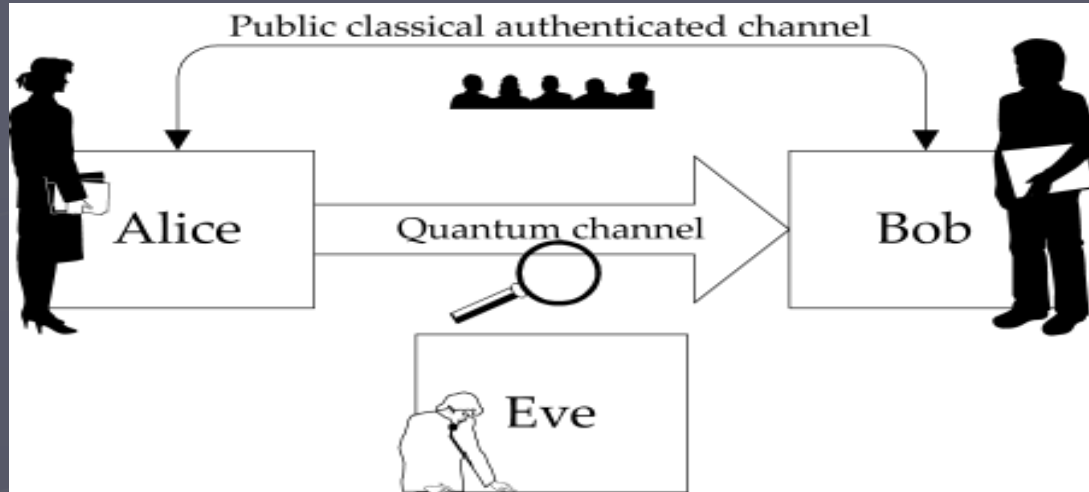
$$(a|0\rangle + b|1\rangle) |0\rangle \rightarrow a|0\rangle |0\rangle + b|1\rangle |1\rangle$$



# Quantum computing

- ▶ In principle qubit-based computers allow massively parallel calculations (each element of superposition acts as a separate process).
- ▶ Current state-of-the-art: 4-qubit superconducting chip from University of California, Santa Barbara (UCSB)
- ▶ Problem is "decoherence", i.e. effective "measurement" of quantum state by unwanted correlation with environment.
- ▶ Target for practical use:  $\sim 100$  qubits (few years time?)
- ▶ Aim is to produce faster algorithms than possible on classical computers, for a given size of problem  $N$  (e.g. number of bits in input data).
- ▶ Algorithms developed as exercise in theory, e.g.
  - 1994: Shor's algorithm: factorises large integers (would break many common high-security cryptography systems).  $t \propto \log(N)^3$  for quantum computer, vs  $t \propto \exp(\log N / 3)$  for best classical algorithm.
  - 1996: Grover's algorithm: database search  $t \propto N^{1/2}$  quantum vs  $t \propto N$  classical

# Quantum cryptography



- ▶ To send secure message from A to B, even if message is intercepted by evesdroppers:
- ▶ Choose private key (very long binary number: for complete security, needs to be as long as the message.)
- ▶ Use to encode message
- ▶ Send message to B
- ▶ B must get key without any possibility of evesdropping.
- ▶ Quantum Key Distribution (QKD) allows this, or rather, allows Eve to be unambiguously detected.

# Quantum Key Distribution

- ▶ Key idea: if Eve reads the key, she makes a measurement and hence disturbs the message. Hence even if she forwards message on, her interference can be detected.
- ▶ Encode and publically transmit message only when key transmission has been verified.
- ▶ Quantum transmission uses photon polarization state to encode 0 or 1, e.g.

Digit	0	1
"Q" states		—
"U" states	\	/

## BB84 Protocol:

1. Randomly generate digits of key
2. Randomly choose to encode each digit using either Q or U states, & transmit
3. Bob randomly chooses Q or U states to decode. If he gets it wrong, gets random answer as U states are 50:50 superpositions of Q states and vice-versa
4. Alice & Bob exchange list of choice of Q vs U states (via public channel).
5. Keep only cases where they randomly made the same choice (in which case the Bob should get the digit Alice sent, barring interference).
6. Check subsample of digits for interference (Eve or bad transmission).

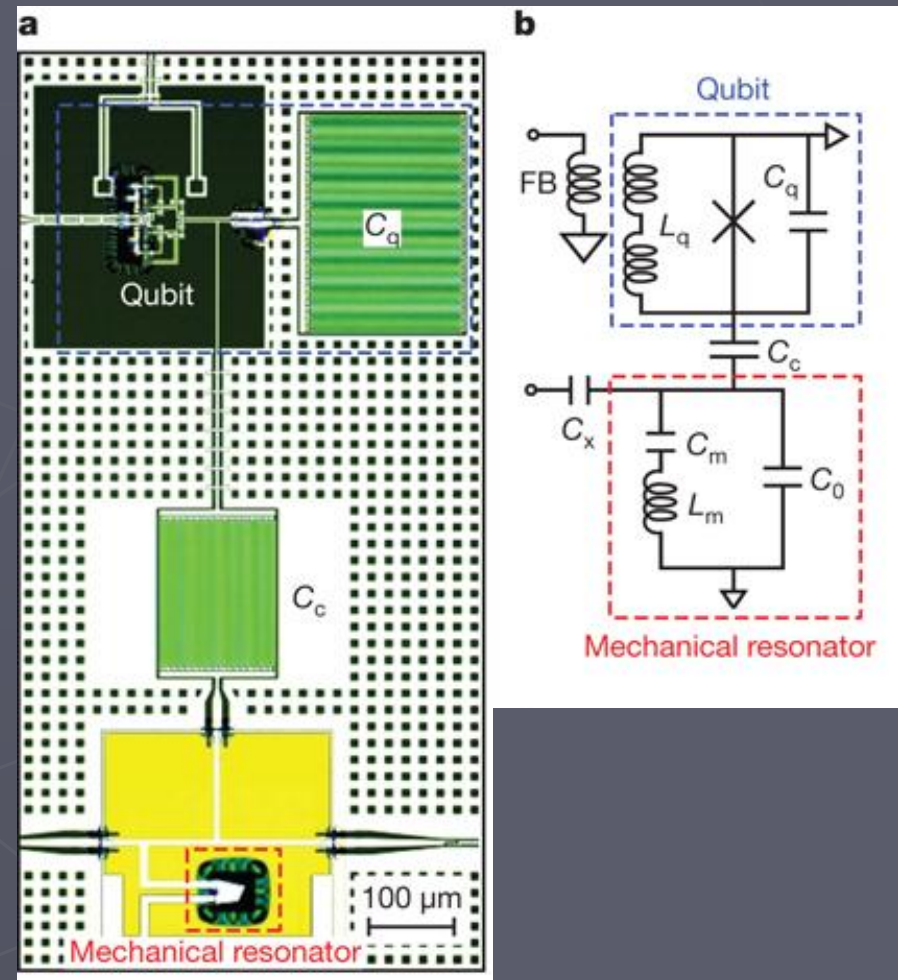
# QKD details

- ▶ What if Eve makes a copy and “measures” that, while forwarding original?
  - Not possible: “Quantum no-cloning theorem” shows that it is impossible to make a perfect copy of an arbitrary unknown quantum state.
- ▶ Can you really do this?
  - YES! There are now several commercial systems
    - ▶ Photons transmitted by optical fibre or free-space transmission
    - ▶ Transmission lengths currently  $> 100$  km



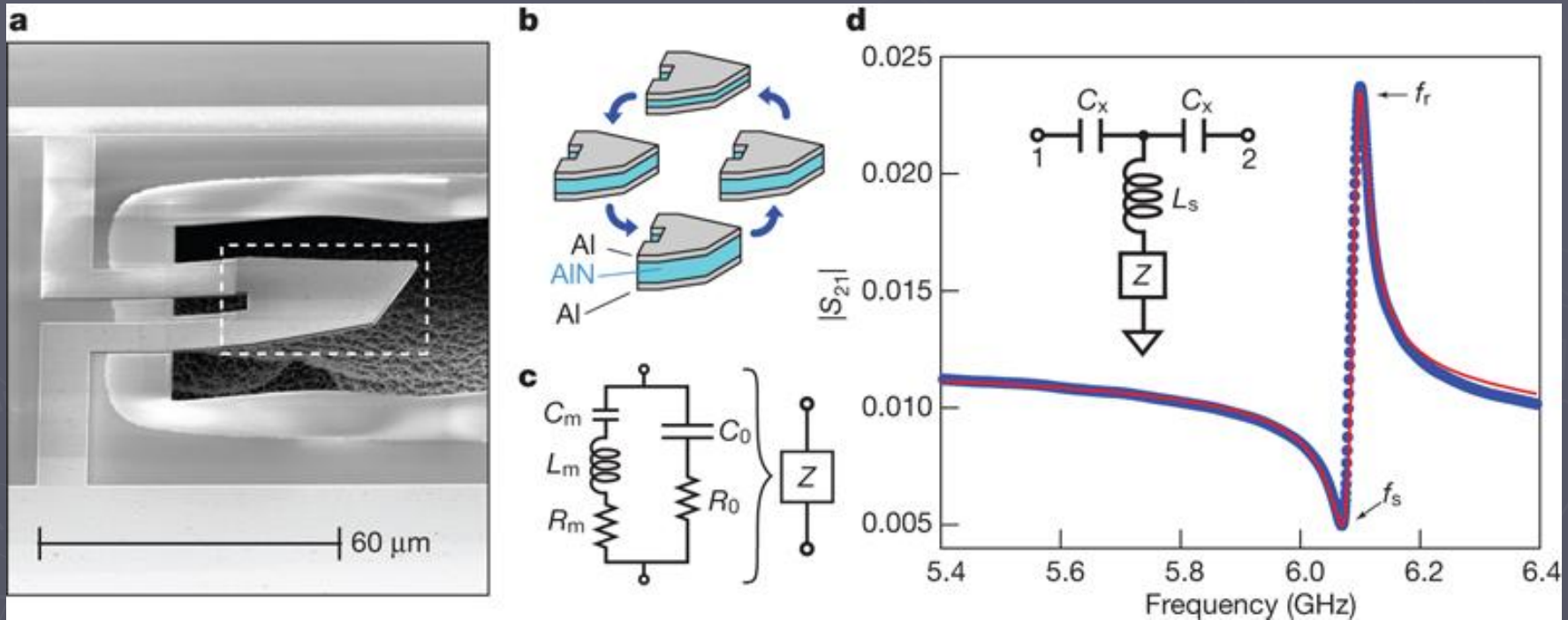
# A Quantum object you can see!

- ▶ Mechanical resonator with a fundamental frequency of 6 GHz
  - Expected to be in ground state for  $T < 0.1$  K
- ▶ Quantum properties demonstrated by electrical coupling to a qubit.
  - Ground and first excited states
  - Superposition of the two
  - Exchange of quantum with qubit
- ▶ Andrew Cleland & John Martinis's team at UCSB (O'Connell et al, *Nature* 2010)
- ▶ Recognized as "Breakthrough of 2010" by *Science* magazine





# Dilatational resonator (Quantum Drum, $Q=260$ )

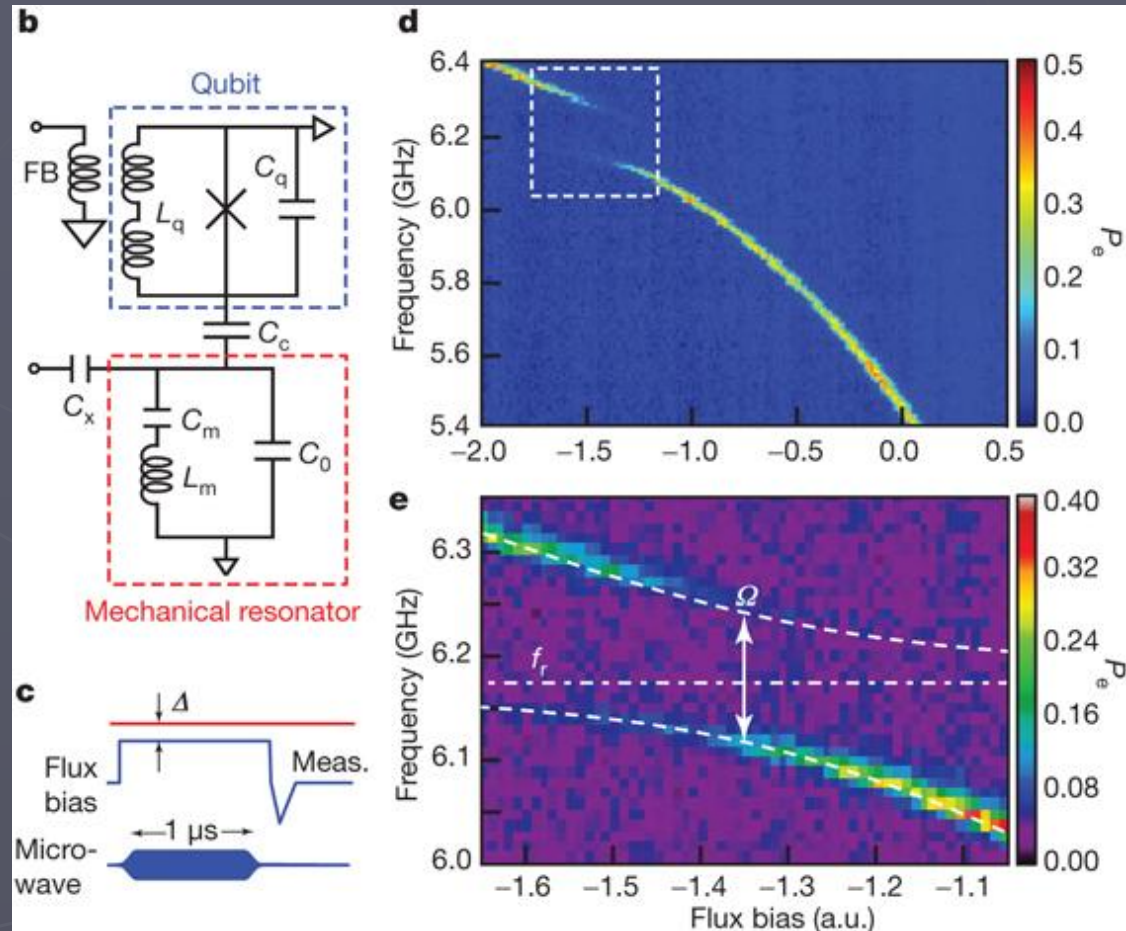


Piezo-electric slab ( $\sim 10^{14}$  atoms) driven/measured by capacitor plates:

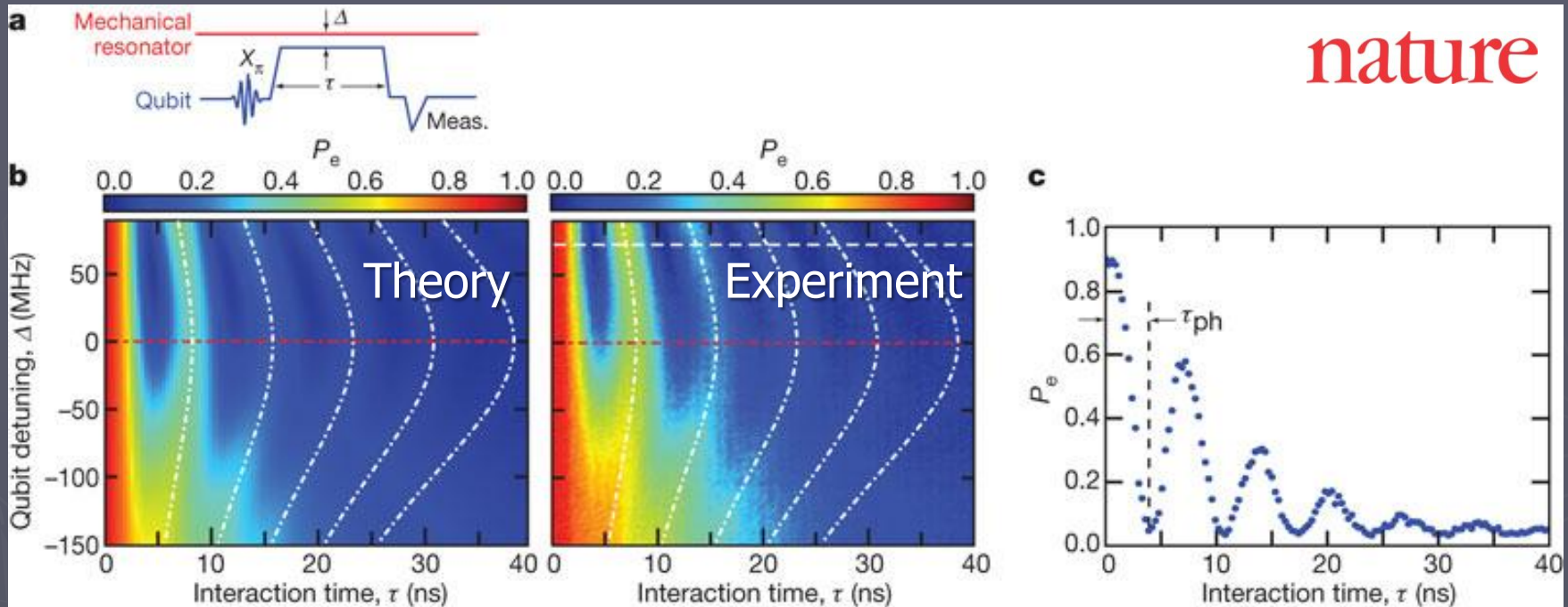
$$2\pi f_r \approx 1/\sqrt{(L_m C_s)}, \quad C_s^{-1} = C_m^{-1} + C_0^{-1}$$

# Coupled qubit–resonator.

- ▶ Qubit has tunable energy difference: vary around energy quantum of oscillator.
- ▶ Repeat  $\sim 1000$  measurements to calculate probability of excited state ( $P_e$ )



# Qubit–resonator swap oscillations



nature

- Excite Qubit with microwave  $X_\pi$  pulse.
- Turn on interaction with resonator for time  $\tau$  by tuning qubit energy to close to resonator frequency (offset =  $\Delta$ )
- Measure  $P_e$  vs  $(\tau, \Delta)$ : the quantum is shunted between qubit & resonator and back:  $|\Psi\rangle = \cos(\pi\tau/\tau_{ph})|e\rangle|0\rangle + \sin(\pi\tau/\tau_{ph})|g\rangle|1\rangle$
- After  $\tau_{ph}$  quantum is in resonator; after  $\tau_{ph}/2$  we have entangled state.