

# Two Goals for Last Lecture

- (1) A few words about *usefulness* of these strange features of QM (entanglement et cetera)
- (2) Just so you don't feel cheated, a few words about the zoo of subatomic particles, antimatter, et cetera -- not so much "concepts" as "botany<sup>1</sup>"...

**Reminder: office hrs tomorrow for review (could schedule another if demand indicates...)**

<sup>1</sup>- (with apologies. Physicists can't help making fun of botany, which we like to misinterpret as "memorizing the names of flowers.")

# Classical Cryptography

The only provably secure way to send secrets:

- the "one-time pad." Alice and Bob share a *random* "key", which is **AS LONG AS THE ENTIRE MESSAGE.**

**They never reuse it. (Soviets made this mistake.)**

**Problem: How to be sure "Eve" didn't get a copy of the key?**

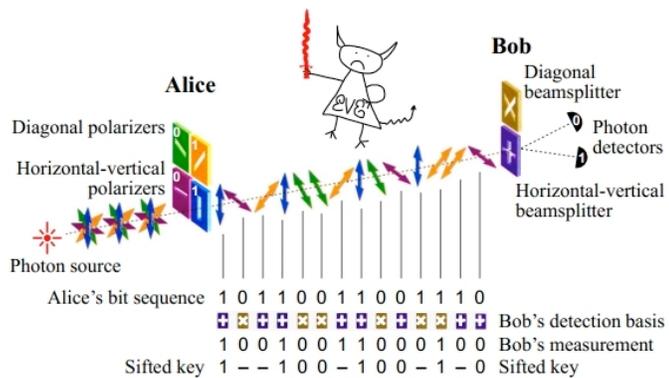


# The Bennett-Brassard Protocol (1984)

**Heisenberg to the rescue!**  
Photons have "polarisation"

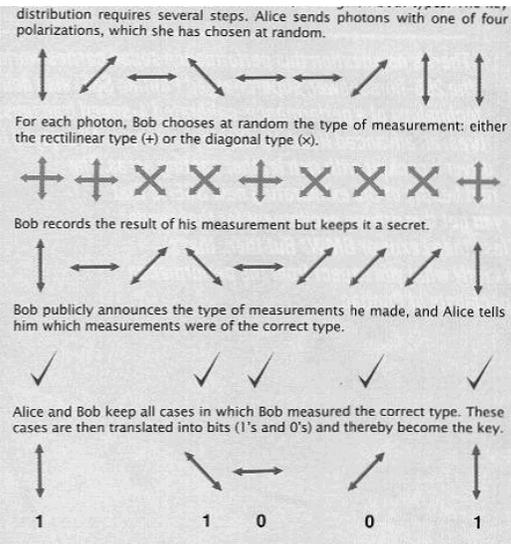
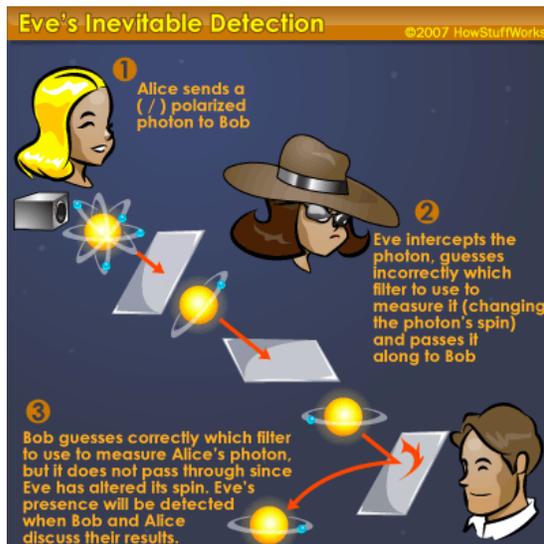
You can measure whether one is  $\updownarrow$  or  $\leftrightarrow$   
OR you can measure whether it's  $\swarrow\searrow$  or  $\nearrow\nwarrow$

But if it's  $\swarrow\searrow$  and you measure HV, the result is random; and vice versa.  $\leftrightarrow$



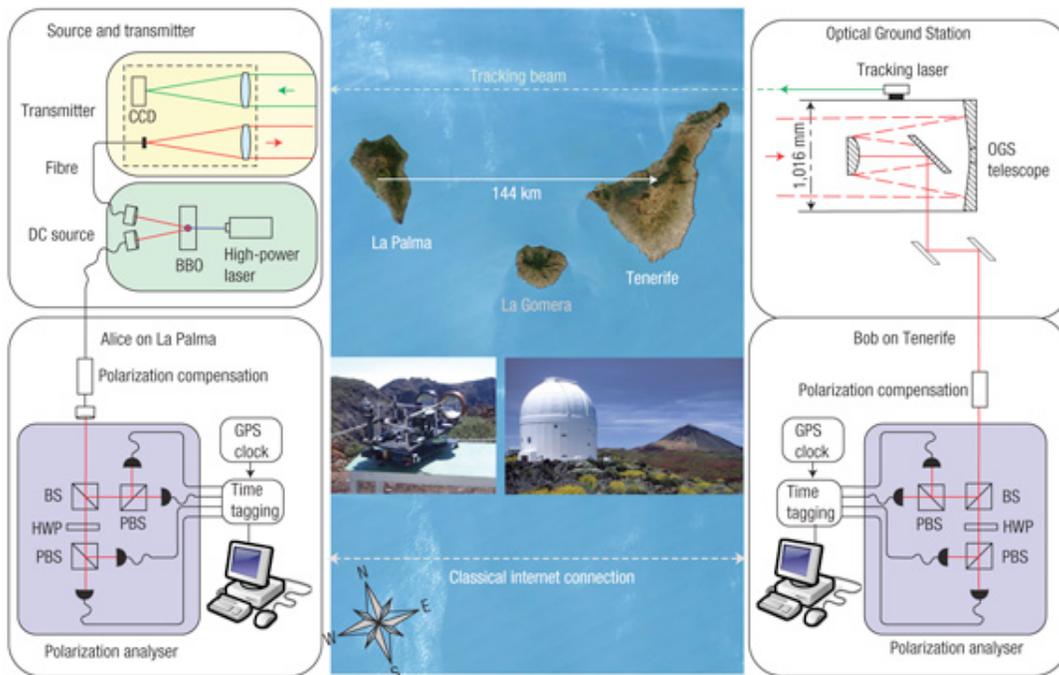
**Eve can't know in advance which axis to measure along... and if she guesses wrong, she destroys the correlations Alice & Bob test.**

# Quantum communications



- Measurement disturbance -> if Eve measures the unknown quantity, there is a detectable effect
- Incompatible observables -> there is always at least one unknown quantity
- No-cloning -> she can't just make a second copy and wait to measure later

# A good excuse for a junket!



mardi 4 décembre 12

5

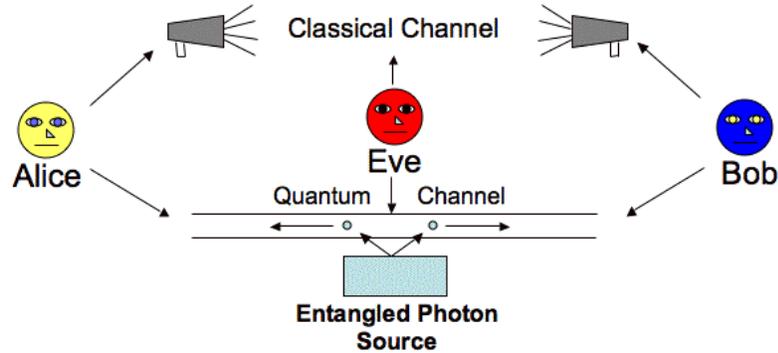
## One slight problem: “side channels”

the device that operated the switch in the first demonstration was so noisy that the system was only “secure against an eavesdropper who happened to be blind and deaf”

mardi 4 décembre 12

6

# Solution: Ekert Protocol



In any basis, Alice and Bob see correlated (opposite) results.  
They can construct a key just as in the Bennett-Brassard '84 protocol

They can use Bell Inequalities to test that their photons are entangled

Recall what BI's really test: could you explain your results with local hidden variables?

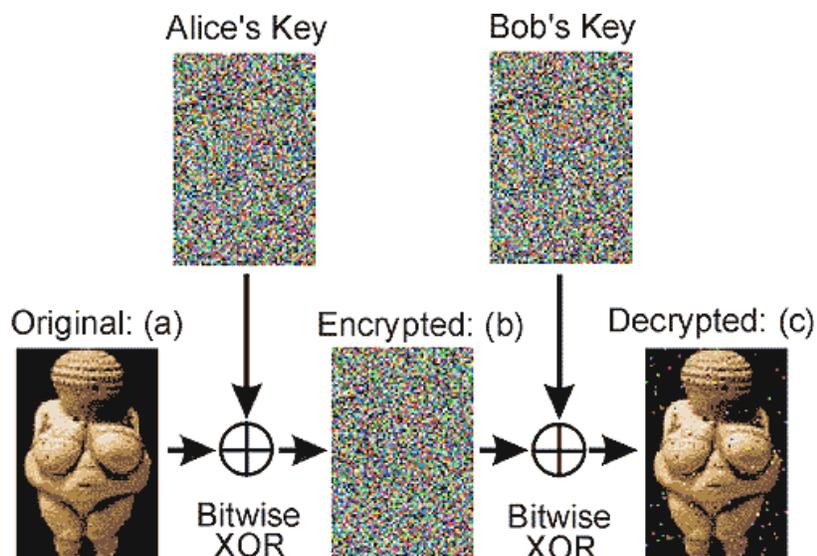
Well, if Eve had measured the photons, each would have "collapsed" to the outcome of some measurement. Eve has the hidden variable.

*If BI's are violated, you know Eve has no information, side channels or not!*

mardi 4 décembre 12

7

# This random string of bits can be used as a secret key...



mardi 4 décembre 12

8

# Quantum Cryptography

Copyright 2003 by Randy Glasbergen.  
www.glasbergen.com



**"We don't need to worry about information security or message encryption. Most of our communications are impossible to understand in the first place."**

mardi 4 décembre 12

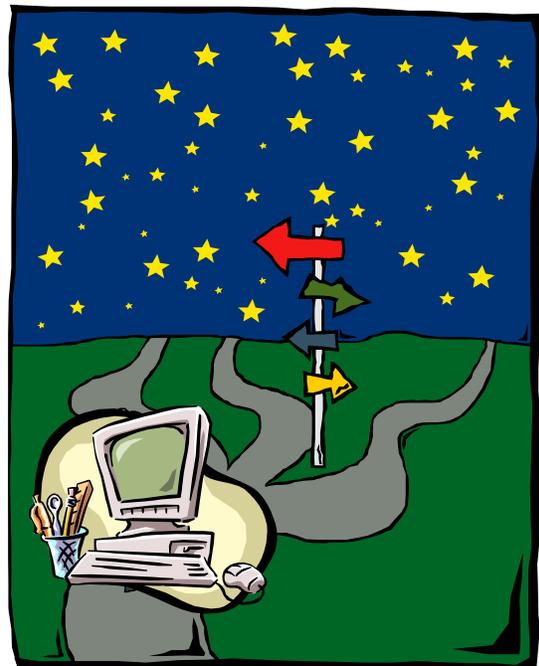
9

## A few words about Quantum Computation...

People like Richard Feynman and David Deutsch realized that the "uncertain" state of a quantum computer could actually be useful...

If it doesn't know what state it's in, maybe it can be in all of them at the same time... and then solve many possible problems all at once?!

(Yes and no, but Deutsch – and later Shor – showed there were at least some clever things to do.)



mardi 4 décembre 12

10

# Quantum Computation?

Some problems (like factoring large numbers) are "exponentially hard" on classical computers [as far as we know] – this means that every time you make the number one digit longer, the problem takes twice [for example] as long for a computer to solve.

**This is why your credit card # is (maybe) secure when you send it over the internet!**

**But there are countless examples throughout history of people who thought their codes were secure, but learned otherwise (see Simon Singh's "The Code Book").**

**Feynman noticed that figuring out what a quantum system is going to do is also exponentially hard... does that mean that (unlike classical computers), the quantum system is “powerful” enough to “simulate” these other hard problems?**

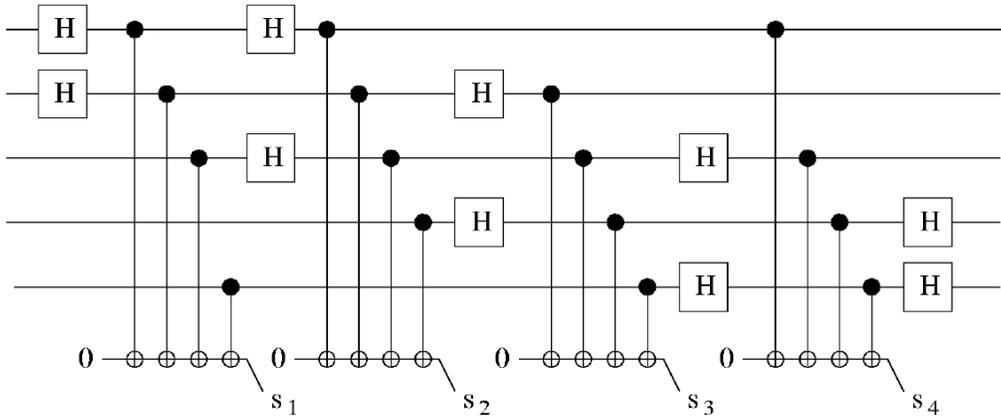
# Quantum Larceny?

Peter Shor showed about eighteen years ago that if a computer were in a *quantum* state (completely uncertain), it could break the classical code (“RSA”) based on factoring products of primes.

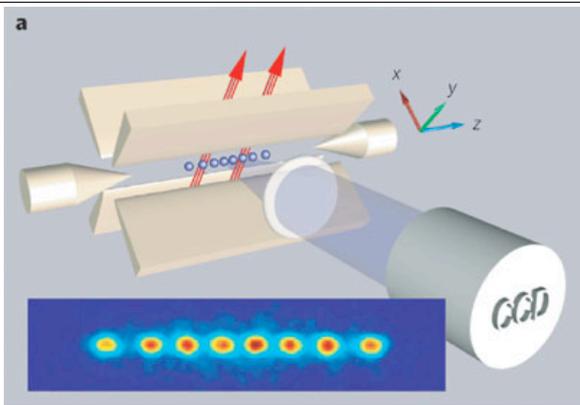
**No solution but quantum cryptography!**



# Quantum computing so far...



This is a small fragment of the "quantum logic circuit" which was used a few years back to prove  $15 = 3 (\pm 1) \cdot 5 (\pm 1) !$



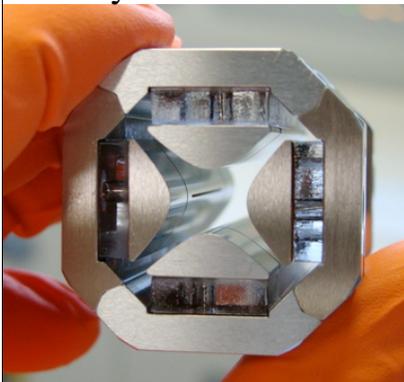
## Wineland's ion-trap quantum computers

(Note: entanglement is the key)

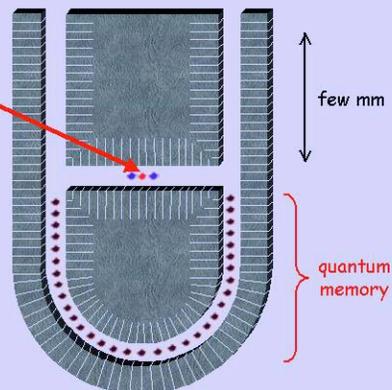
In a few more years?

Scalable Ion Trap Quantum Computer

Today



"refrigerator" ions suppress motional decoherence



# The “standard model” (mostly)

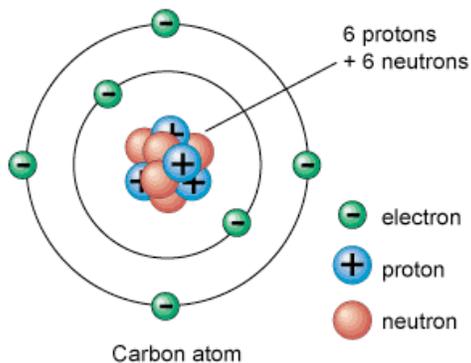
## Periodic Table of Elements

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	<b>H</b> Hydrogen 1.00794																	
2	<b>Li</b> Lithium 6.941	<b>Be</b> Beryllium 9.012182																
3	<b>Na</b> Sodium 22.98976928	<b>Mg</b> Magnesium 24.304																
4	<b>K</b> Potassium 39.0983	<b>Ca</b> Calcium 40.078	<b>Sc</b> Scandium 44.955912	<b>Ti</b> Titanium 47.887	<b>V</b> Vanadium 50.9415	<b>Cr</b> Chromium 51.9961	<b>Mn</b> Manganese 54.938044	<b>Fe</b> Iron 55.845	<b>Co</b> Cobalt 58.933195	<b>Ni</b> Nickel 58.6934	<b>Cu</b> Copper 63.546	<b>Zn</b> Zinc 65.38	<b>Ga</b> Gallium 69.723	<b>Ge</b> Germanium 72.64	<b>As</b> Arsenic 74.9216	<b>Se</b> Selenium 78.96	<b>Br</b> Bromine 79.904	<b>Kr</b> Krypton 83.798
5	<b>Rb</b> Rubidium 85.4678	<b>Sr</b> Strontium 87.62	<b>Y</b> Yttrium 88.90584	<b>Zr</b> Zirconium 91.224	<b>Nb</b> Niobium 92.90638	<b>Mo</b> Molybdenum 95.94	<b>Tc</b> Technetium 98.90625	<b>Ru</b> Ruthenium 101.07	<b>Rh</b> Rhodium 102.90550	<b>Pd</b> Palladium 106.42	<b>Ag</b> Silver 107.8682	<b>Cd</b> Cadmium 112.411	<b>In</b> Indium 114.818	<b>Sn</b> Tin 118.710	<b>Sb</b> Antimony 121.757	<b>Te</b> Tellurium 127.60	<b>I</b> Iodine 126.905	<b>Xe</b> Xenon 131.29
6	<b>Cs</b> Cesium 132.90545196	<b>Ba</b> Barium 137.327	<b>La</b> Lanthanum 138.9048	<b>Hf</b> Hafnium 178.49	<b>Ta</b> Tantalum 180.94788	<b>W</b> Tungsten 183.84	<b>Re</b> Rhenium 186.207	<b>Os</b> Osmium 190.23	<b>Ir</b> Iridium 192.222	<b>Pt</b> Platinum 195.084	<b>Au</b> Gold 196.966569	<b>Hg</b> Mercury 200.59	<b>Tl</b> Thallium 204.3833	<b>Pb</b> Lead 207.2	<b>Bi</b> Bismuth 208.9804	<b>Po</b> Polonium 209	<b>At</b> Astatine 210	<b>Rn</b> Radon 222.01753
7	<b>Fr</b> Francium 223	<b>Ra</b> Radium 226	<b>Rf</b> Rutherfordium 261	<b>Db</b> Dubnium 262	<b>Sg</b> Seaborgium 263	<b>Bh</b> Bohrium 264	<b>Hs</b> Hassium 277	<b>Mt</b> Meitnerium 268	<b>Ds</b> Darmstadtium 271	<b>Rg</b> Roentgenium 272	<b>Cn</b> Copernicium 285	<b>Uub</b> Ununbium 286	<b>Uut</b> Ununtrium 287	<b>Uuq</b> Ununquadium 288	<b>Uup</b> Ununpentium 289	<b>Uuh</b> Ununhexium 290	<b>Uus</b> Ununseptium 291	<b>Uuo</b> Ununoctium 294

For elements with no stable isotopes, the mass number of the isotope with the longest half-life is in parentheses.

Design and Interface Copyright © 1997 Michael Dayah (michael@dayah.com), <http://www.ptable.com/>

# The “standard model” (mostly)





# The "standard model" (mostly)

Standard Model of  
**FUNDAMENTAL PARTICLES AND INTERACTIONS**

The Standard Model summarizes the current knowledge in Particle Physics. It is the quantum theory that includes the theory of strong interactions (quantum chromodynamics or QCD) and the unified theory of weak and electromagnetic interactions (electroweak). Gravity is included on this chart because it is one of the fundamental interactions even though not part of the "Standard Model."

**FERMIONS**  
matter constituents  
spin = 1/2, 3/2, 5/2, ...

Leptons			Quarks		
Flavor	Mass GeV/c <sup>2</sup>	Electric charge	Flavor	Approx. Mass GeV/c <sup>2</sup>	Electric charge
$\nu_e$ electron neutrino	<1·10 <sup>-6</sup>	0	u up	0.003	2/3
e electron	0.000511	-1	d down	0.006	-1/3
$\nu_\mu$ muon neutrino	<0.0002	0	c charm	1.3	2/3
$\mu$ muon	0.106	-1	s strange	0.1	-1/3
$\nu_\tau$ tau neutrino	<0.02	0	t top	175	2/3
$\tau$ tau	1.7771	-1	b bottom	4.3	-1/3

Spin is the intrinsic angular momentum of particles. Spin is given in units of  $\hbar$ , which is the quantum unit of angular momentum, where  $\hbar = h/2\pi = 6.58 \cdot 10^{-27} \text{ GeV} \cdot \text{s} = 1.05 \cdot 10^{-34} \text{ J} \cdot \text{s}$ .

Electric charges are given in units of the proton's charge. In SI units the electric charge of the proton is  $1.60 \cdot 10^{-19}$  coulombs.

The energy unit of particle physics is the electronvolt (eV), the energy gained by one electron by crossing a potential difference of one volt. Masses are given in GeV/c<sup>2</sup> (remember  $E = mc^2$ , where  $1 \text{ GeV} = 10^9 \text{ eV} = 1.60 \cdot 10^{-10} \text{ joule}$ ). The mass of the proton is  $0.938 \text{ GeV}/c^2 = 1.67 \cdot 10^{-27} \text{ kg}$ .

**BOSONS**  
force carriers  
spin = 0, 1, 2, ...

Unified Electroweak			Strong (color)		
Name	Mass GeV/c <sup>2</sup>	Electric charge	Name	Mass GeV/c <sup>2</sup>	Electric charge
$\gamma$ photon	0	0	g gluon	0	0
$W^+$	80.4	-1			
$W^-$	80.4	+1			
$Z^0$	91.187	0			

**Color Charge**  
Each quark carries one of three types of "strong charge," also called "color charge." These charges have nothing to do with the color of visible light. There are eight possible types of color charge for gluons, and a selected color-charged particles interact by exchanging photons, in strong interactions color-charged particles interact by exchanging gluons. Leptons, photons, and  $W$  and  $Z$  bosons have no strong interactions and hence no color charge.

**Quarks Confined in Mesons and Baryons**  
One cannot isolate quarks and gluons; they are confined to color-neutral particles called hadrons. This confinement (binding) results from multiple exchanges of gluons among the color-charged constituents. As color-charged particles (quarks and gluons) move apart, the energy in the color-force field between them increases. This energy eventually is converted into additional quark-antiquark pairs (see Figure below). The quarks and antiquarks that combine into hadrons, these are the particles seen to emerge. Two types of hadrons have been observed in nature: mesons ( $q\bar{q}$ ) and baryons ( $qqq$ ).

**Residual Strong Interaction**  
The strong binding of color-neutral protons and neutrons to form nuclei is due to residual strong interactions between their color-charged constituents. It is similar to the residual electrical interaction that binds electrically neutral atoms to form molecules. It can also be viewed as the exchange of mesons between the hadrons.

**Structure within the Atom**

If the protons and neutrons in this picture were 10 cm across, then the quarks and electrons would be less than 11 microns and the entire atom would be about 10 km across.

**PROPERTIES OF THE INTERACTIONS**

Property	Interaction	Gravitational	Weak (Electroweak)	Electromagnetic	Strong
		Mass-Energy	Flavor	Electric Charge	Color Charge
Acts on:	All	All	Quarks, Leptons	Electrically charged	Quarks, Gluons
Particles experiencing:	All	Quarks, Leptons	Electrically charged	Quarks, Gluons	Hadrons
Particles mediating:	Graviton (not yet observed)	$W^+$ , $W^-$ , $Z^0$	$\gamma$	Gluons	Mesons
Strength (relative to electrom.)	$10^{-41}$	0.8	1	60	Not applicable to quarks
Range	$10^{-16}$ m	$10^{-16}$ m	$10^{-16}$ m	Not applicable to hadrons	20
Two protons in nucleus	$10^{-36}$	$10^{-7}$	1	Not applicable to hadrons	20

**Baryons  $qqq$  and Antibaryons  $\bar{q}\bar{q}\bar{q}$**   
Baryons are fermionic hadrons. There are about 100 types of baryons.

Symbol	Name	Quark content	Electric charge	Mass GeV/c <sup>2</sup>	Spin
p	proton	uud	1	0.938	1/2
$\bar{p}$	anti-proton	$\bar{u}\bar{u}\bar{d}$	-1	0.938	1/2
n	neutron	udd	0	0.940	1/2
$\bar{n}$	anti-neutron	$\bar{u}\bar{d}\bar{d}$	0	0.940	1/2
$\Lambda$	lambda	uds	0	1.116	1/2
$\Sigma^+$	sigma	uus	1	1.072	1/2

**Mesons  $q\bar{q}$**   
Mesons are bosonic hadrons. There are about 100 types of mesons.

Symbol	Name	Quark content	Electric charge	Mass GeV/c <sup>2</sup>	Spin
$\pi^+$	pion	$u\bar{d}$	+1	0.140	0
$K^-$	kaon	$s\bar{u}$	-1	0.494	0
$\rho^+$	rho	$u\bar{d}$	+1	0.770	1
$B^0$	B meson	$d\bar{b}$	0	5.279	0
$\eta_c$	eta	$c\bar{c}$	0	2.380	0

**Matter and Antimatter**  
For every particle type there is a corresponding antiparticle type, denoted by a bar over the particle symbol (unless  $\nu$  or  $\bar{\nu}$  charge is shown). Particle and antiparticle have identical mass and spin but opposite charges. Some electrically neutral bosons (e.g.  $Z^0$ ,  $\gamma$ , and  $\eta$ , but not  $K^0$  or  $D^0$ ) are their own antiparticles.

**Figures**  
These diagrams are an artist's conception of physical processes. They are not exact and have no meaningful scale. Green shaded areas represent the cloud of gluons or the gluon field, and red lines the quark paths.

$n \rightarrow p + e^- + \bar{\nu}_e$

A neutron decays to a proton, an electron, and an antineutrino via a virtual (mediating) boson. This reaction is decay.

$e^- + e^+ \rightarrow \gamma + \gamma$

An electron and positron annihilate into two photons. This reaction is annihilation.

$p + p \rightarrow 2p + 2p + \text{associated hadrons}$

Two protons colliding at high energy can produce various hadrons plus one or two mesons. Particles such as  $Z$  bosons, leptons such as this one are rare but can yield vital clues to the structure of matter.

**The Particle Adventure**  
Visit the award-winning web feature The Particle Adventure at <http://ParticleAdventure.org>

This chart has been made possible by the generous support of:  
U.S. Department of Energy  
U.S. National Science Foundation  
Lawrence Berkeley National Laboratory  
Stanford Linear Accelerator Center  
American Physical Society, Division of Particles and Fields  
BURLIE INDUSTRIES, INC.

©2006 Contemporary Physics Education Project, CPEP is a non-profit organization of teachers, physicists, and students. We are grateful to CPEP, NSL, SLAC, Lawrence Berkeley National Laboratory, Berkeley, CA, USA for contribution on charts, test materials, hardware, classroom activities, and workshops. See <http://CPEPweb.org>

## Why does "high-energy physics" = "particle physics" ?

**Structure within the Atom**

If the protons and neutrons in this picture were 10 cm across, then the quarks and electrons would be less than 0.1 mm in size and the entire atom would be about 10 km across.

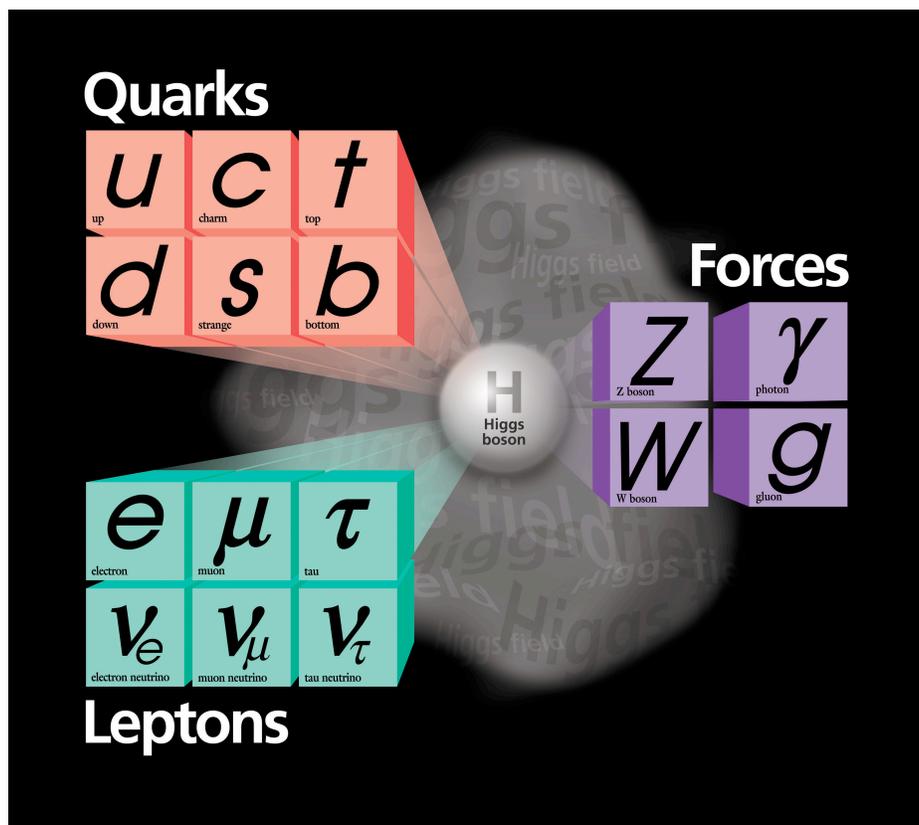
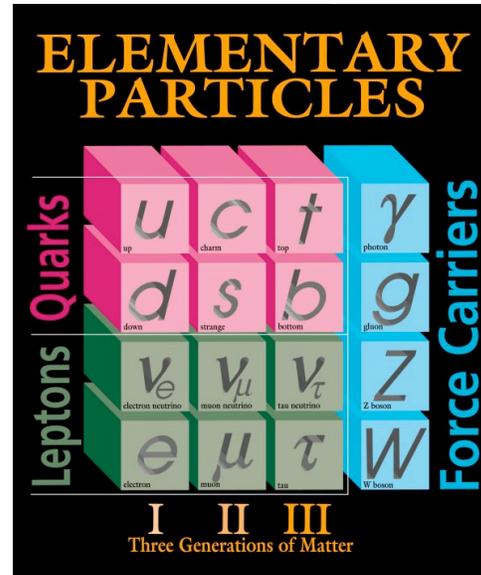
Uncertainty principle: things confined to small regions may have very large momenta -> high energies.

It takes a lot of energy to build a good "microscope."

# Matter is electrons + protons (quarks) + neutrons (quarks).

1936: studying cosmic rays, people found particles which behaved just like electrons, but hundreds of times heavier: “muons.”

1937: atomic physicist I. I. Rabi asks “who ordered that?”



# How to do QM *and* relativity?

**Wait a minute:**

**in relativity, space & time are like two aspects of one thing; they need to be treated “symmetrically.”**

**But QM said “there is some  $\Psi(x)$  given at  $t=0$ ; find it for other  $t$ .”**

**Not symmetric.**

**Schrödinger found a symmetric equation, but it gave the wrong answers (turns out to be correct for “pions,” not for electrons, I think).**

**1928 - Dirac finds one that works.**

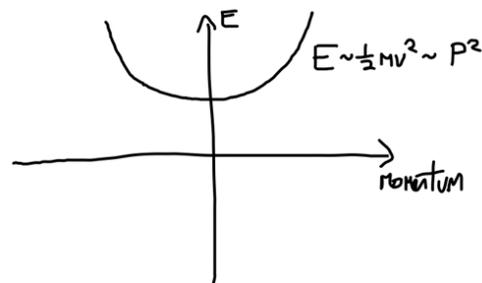
**But a problem...**

## Symmetry of $x$ & $t$

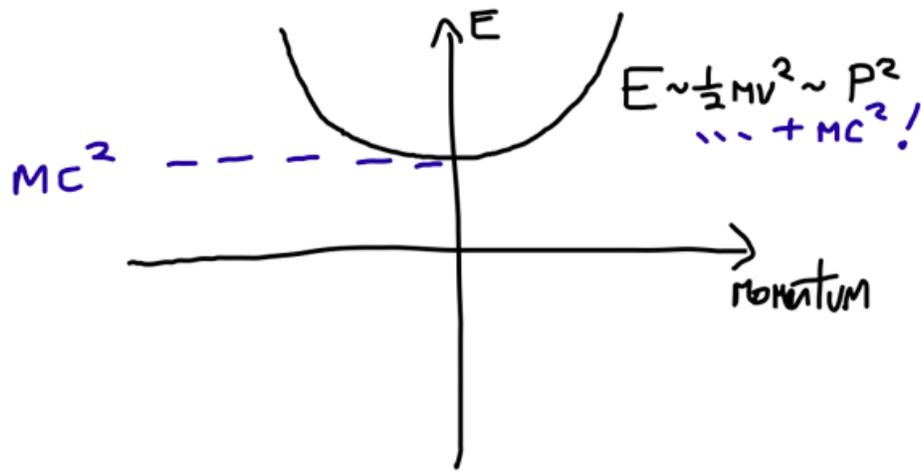
The Schrödinger equation starts from the idea that the energy depends on momentum squared (kinetic energy goes up by 4 if velocity doubles)

It turns out that Energy has to do with time (the frequency of the wave) and Momentum has to do with space (the *wavelength*).

To be symmetric, the equation should either relate  $E^2$  and  $P^2$  or  $E$  and  $P$ , but certainly not  $E$  and  $P^2$  !



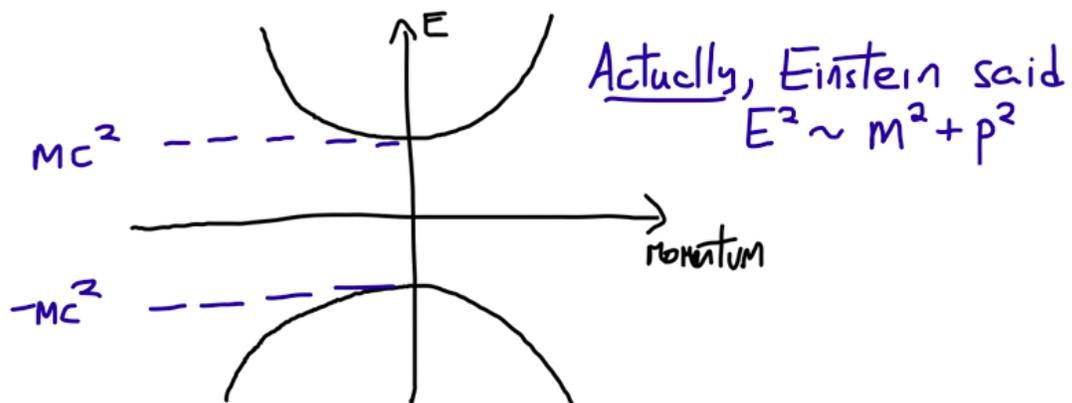
## Remember relativity...



mardi 4 décembre 12

25

## The “symmetric” solution

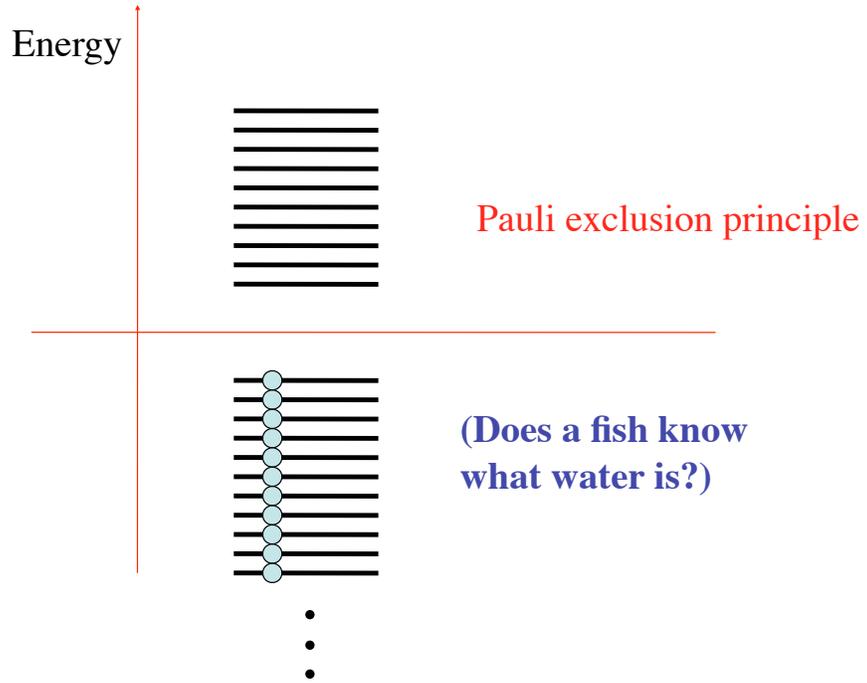


But wait a second: things always flow to lower-energy states. If there are *negative* energy states, with  $E$  all the way down to  $-\infty$ , then why doesn't everything run off to infinity??

mardi 4 décembre 12

26

# Dirac sea?



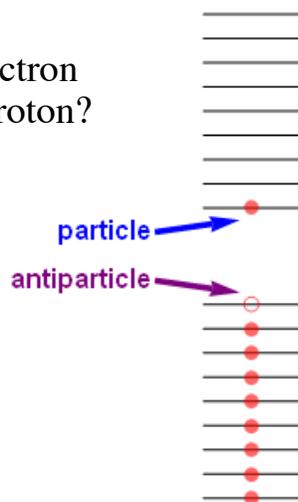
mardi 4 décembre 12

27

# Only when it's missing!

electron  
& proton?

NO!

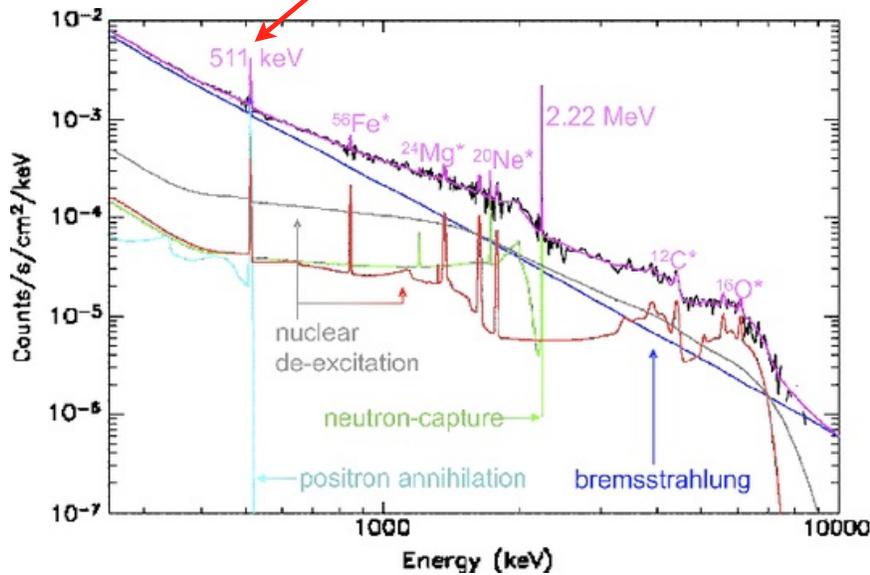


mardi 4 décembre 12

28

# Gamma rays observed from solar flares

511 keV = the electron mass divided by  $c^2$ !



## Problems...

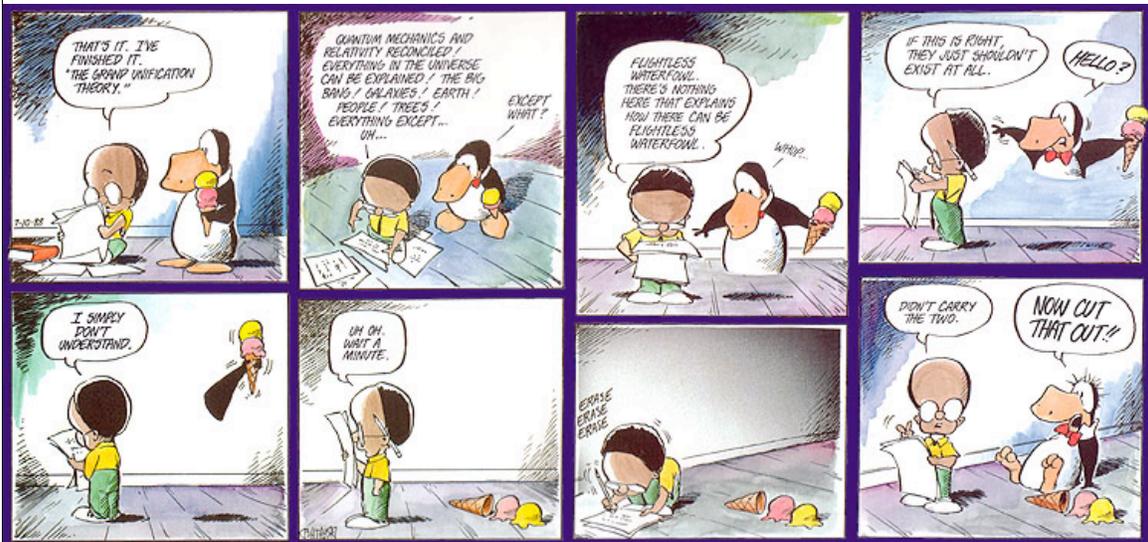
Mass (Higgs?)

Gravity (string theory? loop quantum gravity?)

Symmetries (why these tiny violations of symmetry?)

Why these particular particles, masses, charges,...?

And, of course, flightless waterfowl:



# Summary

“There is more on Heaven and Earth, Horatio, than is dreamt of in your philosophy.”

But that’s not a reason to try to learn as much as we can about it and, whenever possible, to make sense of it.

*This* (not “calculating things,” let alone building things) is the project of physics. (Though we’re kind of chuffed if what we find out also turns out to be useful, naturally!)