Hacking Quantum Cryptography

Marina von Steinkirch
~ Yelp Security

Agenda

1. Quantum Mechanics in 10 mins
2. Quantum Computing in 11 mins
3. Quantum Key Exchange in 100 mins

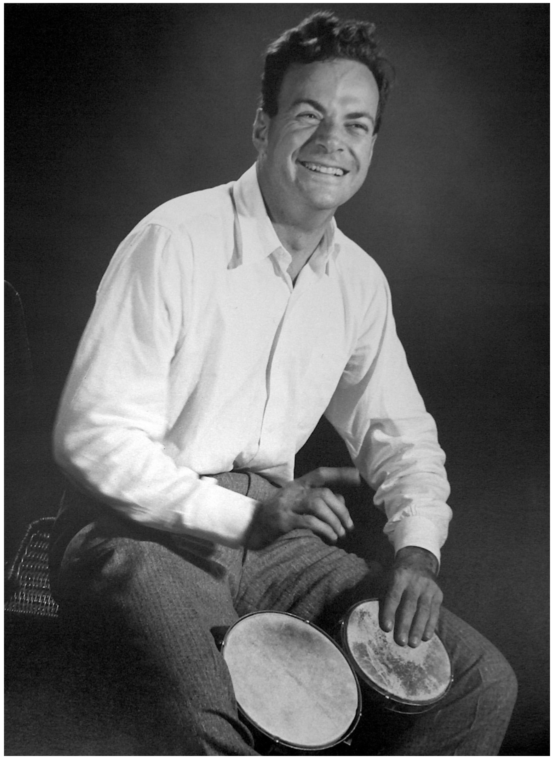
(or more minutes)

Some disclaimers

- This is my personal views and do not necessarily reflect views of my employer.
- This is a physicist point of view.
- For a more in-depth discussion on the privacy issues in the post-quantum crypto paradigm, check out Jennifer Katherine Fernick’s work.

What if we are all just a simulation?

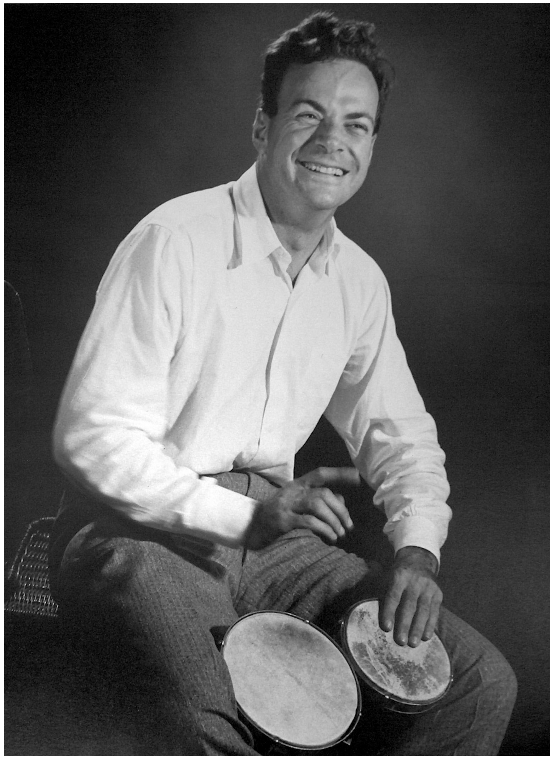
“To simulate reality, in it lowest level, you would need a quantum computer” (Feynman, 1982)



What if we are all just a simulation?

“To simulate reality, in it lowest level, you would need a quantum computer” (Feynman, 1982)

The universe is a 13.8 billion years-old quantum computer.

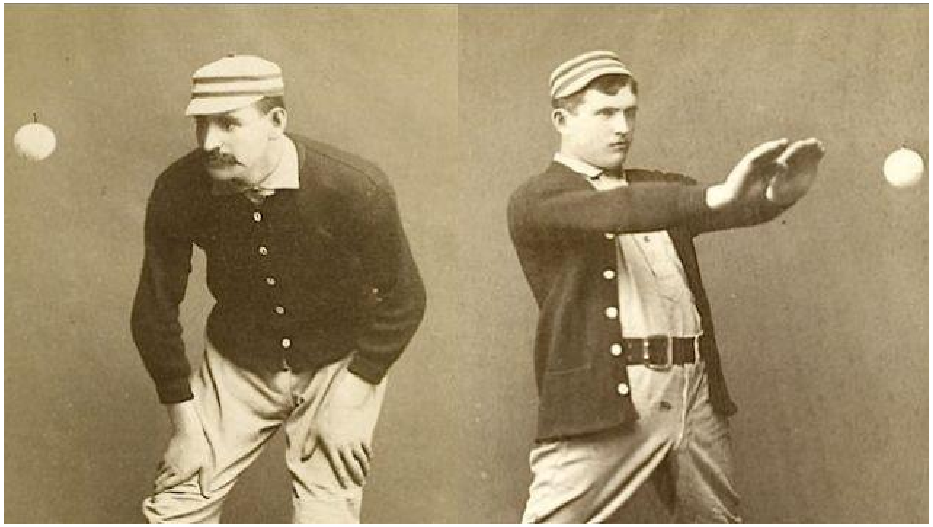


But first, let’s understand how quantum mechanics changed the way we see the world...

It was pretty boring in the 1800s...

"There is nothing new to be discovered in physics now. All that remains is more and more precise measurement."

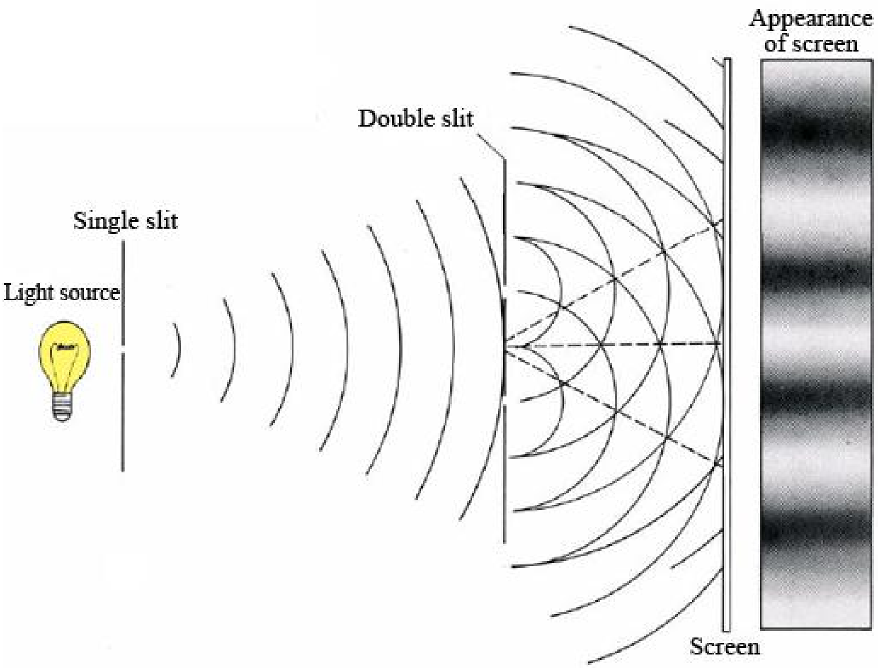
(Lord Kelvin, 1897 - before QM)

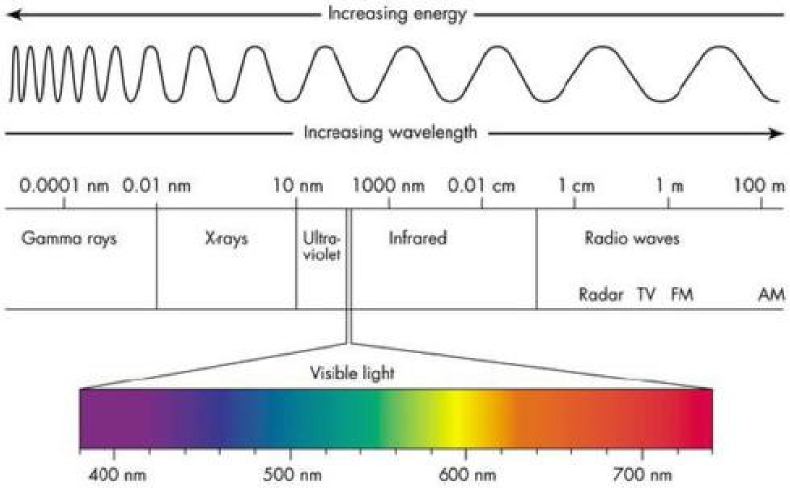


Then… the Ultraviolet Catastrophe

- Early 1800s: light as a wave

(Young’s double slit experiment, 1801)





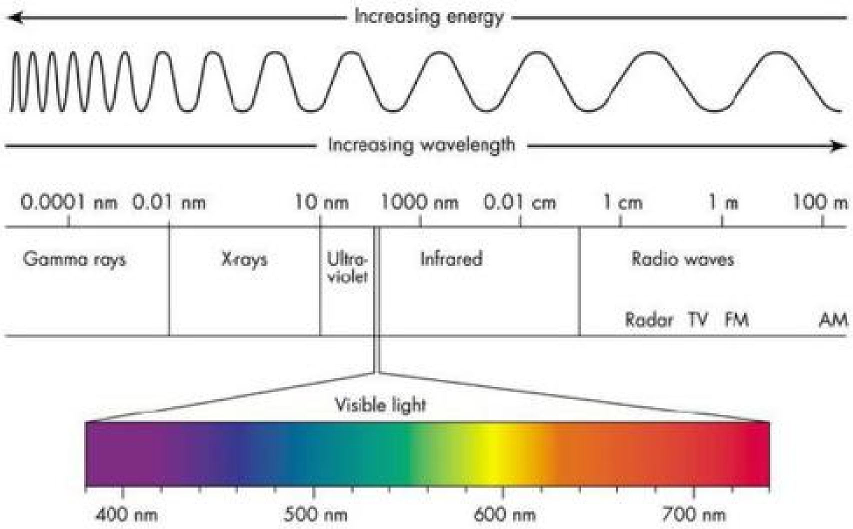
Then... the Ultraviolet Catastrophe

- Early 1800s: light as a wave

(Young's double slit experiment, 1801)

- Classical Thermodynamics: <E> $\propto$ wavelength

(for some temperature)



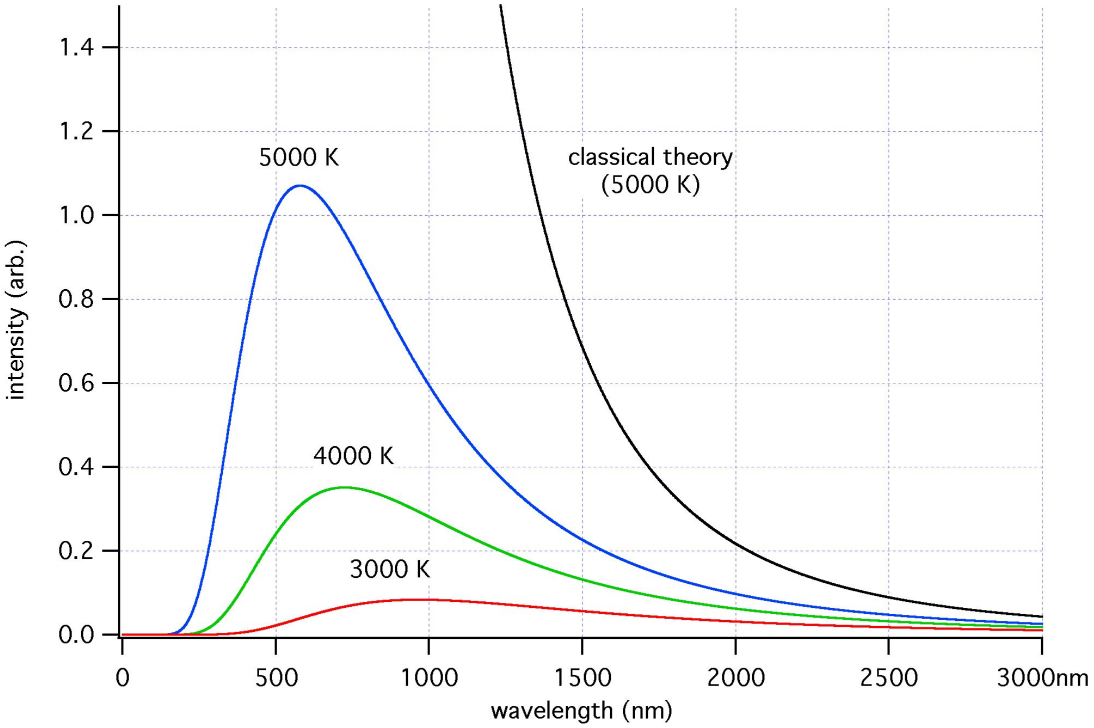
Then... the Ultraviolet Catastrophe

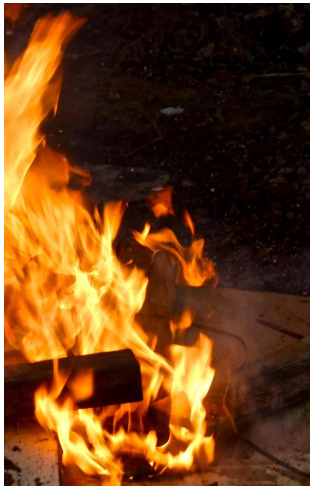
What would happen if radiation was emitted in infinite wavelengths?

?

Then… the Ultraviolet Catastrophe

What would happen if radiation was emitted in infinite wavelengths?





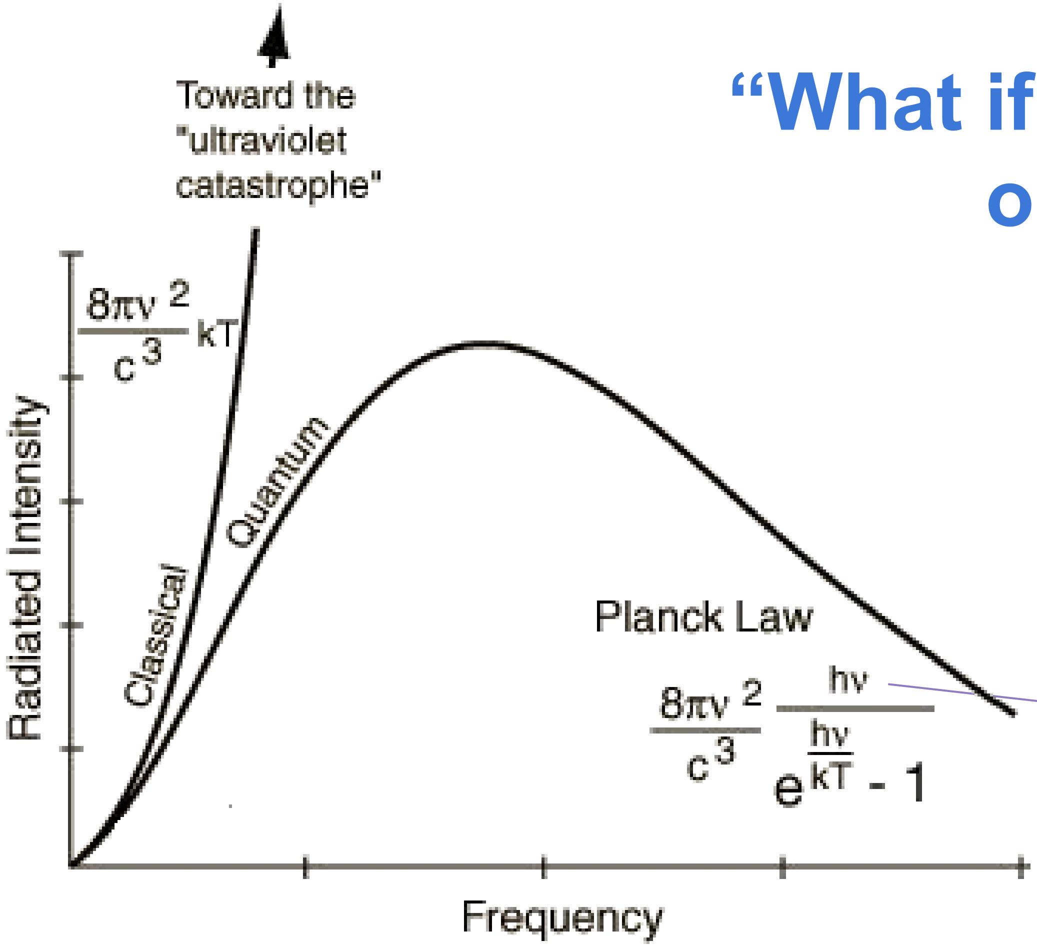
Enter Quantum Mechanics

“What if Energy is released on bundles instead?

Just dunno why :(”

(Max Planck, 1899)

Enter Quantum Mechanics



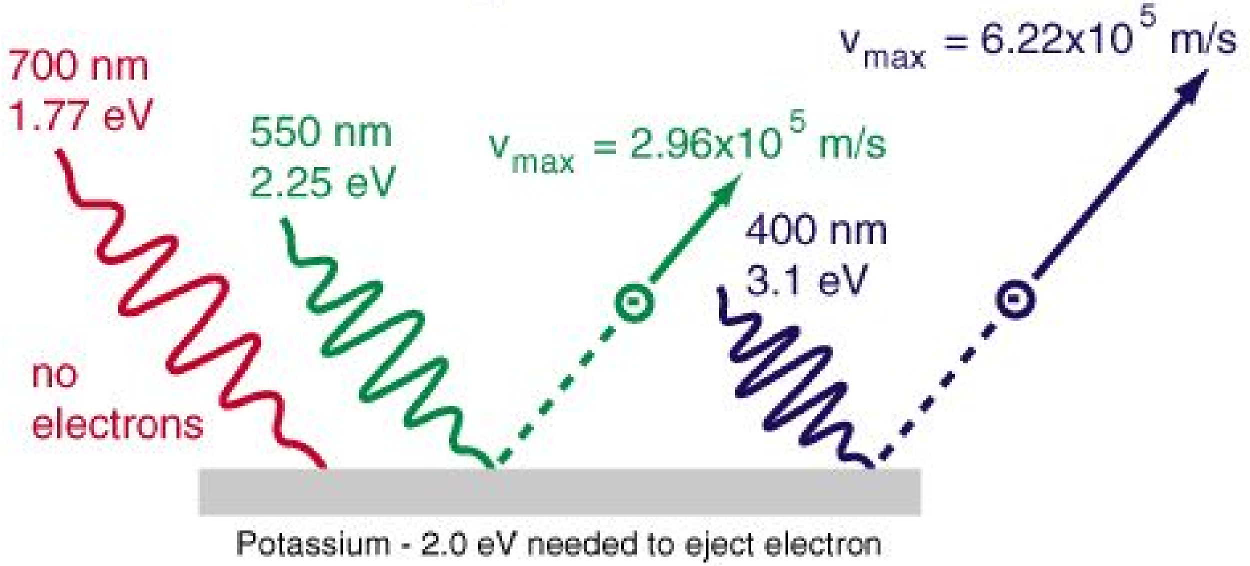
"What if Energy is released on bundles instead? Just dunno why :("

(Max Planck, 1899)

$$\hbar = \frac{h}{2\pi} = 6.6\times10^{-16}\,\mathrm{eV\,s}$$

Particle-Wave Duality

@Qu4ntumPl4nck No worries, dude! #GotThis (Einstein, 1905)


700 nm
1.77 eV
no electrons
550 nm
2.25 eV
$v_{max} = 2.96 \times 10^5$ m/s
400 nm
3.1 eV
$v_{max} = 6.22 \times 10^5$ m/s
Potassium - 2.0 eV needed to eject electron

Photoelectric effect

Particle-Wave Duality

@Qu4ntumPl4nck No worries, dude! #GotThis (Einstein, 1905)

$$E_{photon} = h\nu$$

How about the matter?

"Doh! Everything in the quantum world is both a particle and a wave. #NobelMaterial"

(de Broglie, 1924)

$$\lambda = \frac{h}{p}$$

Wavefunction

Matter is represented by a **wavefunction**, a mathematical probability that represents the quantum state of one or more particles.

$$\psi(x) = A_{+}e^{+i\sqrt{(2mE/\hbar^{2})}x} + A_{-}e^{-i\sqrt{(2mE/\hbar^{2})}x}$$

Wavefunction

Matter is represented by a **wavefunction**, a mathematical probability that represents the quantum state of one or more particles.

$$\psi(x) = A_{+}e^{+i\sqrt{(2mE/\hbar^2)}x} + A_{-}e^{-i\sqrt{(2mE/\hbar^2)}x}$$

Squaring the amplitude gives the probability of that state

Wavefunction

Matter is represented by a **wavefunction**, a mathematical probability that represents the quantum state of one or more particles.

$$|\psi\rangle = a_{\psi}|\uparrow\,\rangle + b_{\psi}|\downarrow\,\rangle$$

Wavefunction

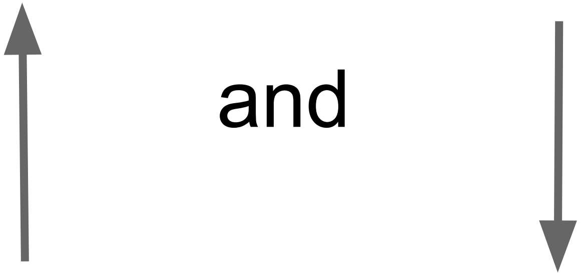
$\psi_{\mathbf{kitty}} = \frac{1}{\sqrt{2}}\psi_{\mathbf{alive}} + \frac{1}{\sqrt{2}}\psi_{\mathbf{dead}}$

(btw, wavefunctions are solutions of the **Schrödinger Equation**, remember, from the half-dead cat?)

$$|\psi\rangle = a_\psi|\uparrow\rangle + b_\psi|\downarrow\rangle$$

What if we take a peak?

Before we observe the state...

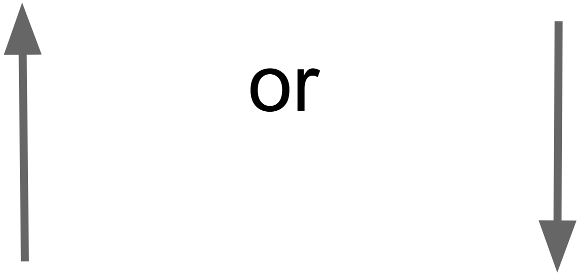


and

(dead and alive)

What if we take a peak?

Observation collapses the probability to the observed state!



or

(dead or alive)

What if we take a peak?

Before we observe the state...

0 and 1

(dead and alive)

What if we take a peak?

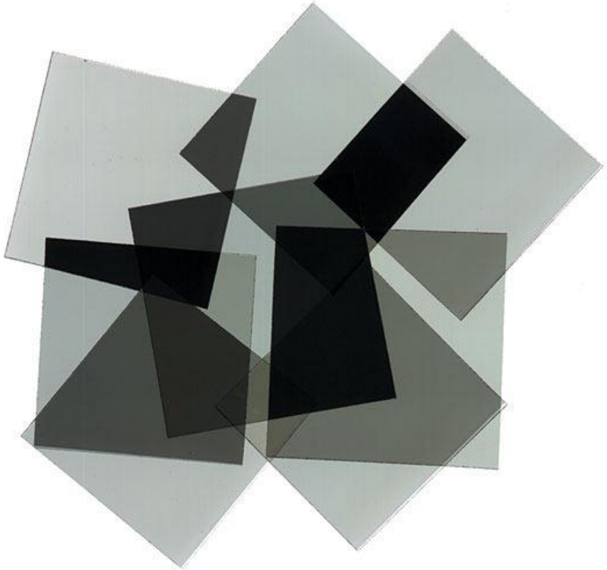
After observing the state…

0 or 1

(dead or alive)

Let's try an experiment

1. 3 Polaroid filters with horizontal, vertical and 45° polarization



Let's try an experiment

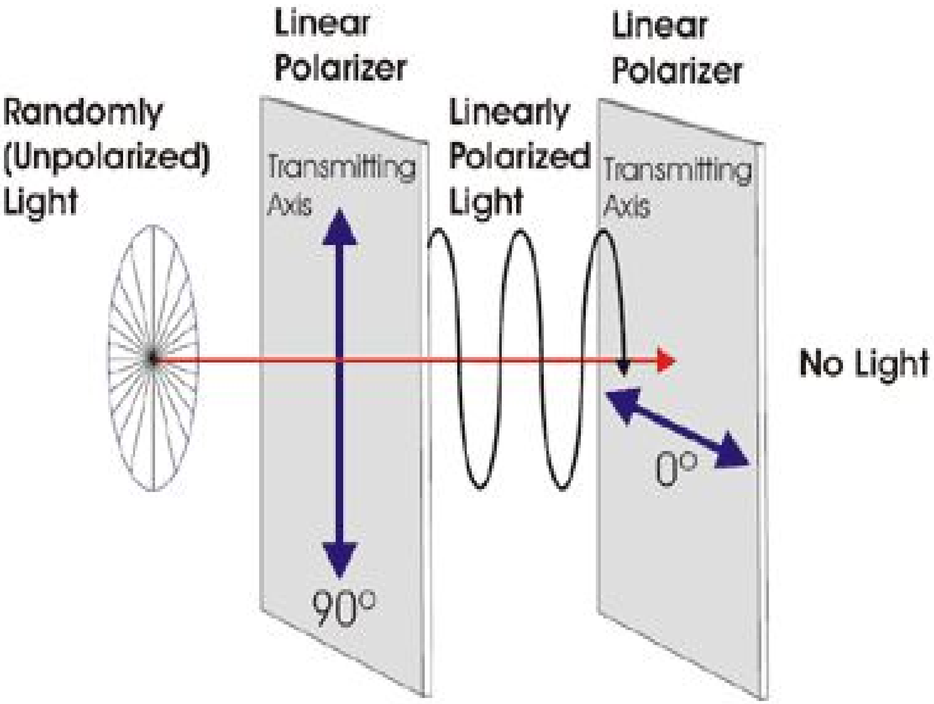
2. Shine light on the horizontal filter

Let's try an experiment

2. Shine light on the horizontal filter → light becomes horizontally polarized

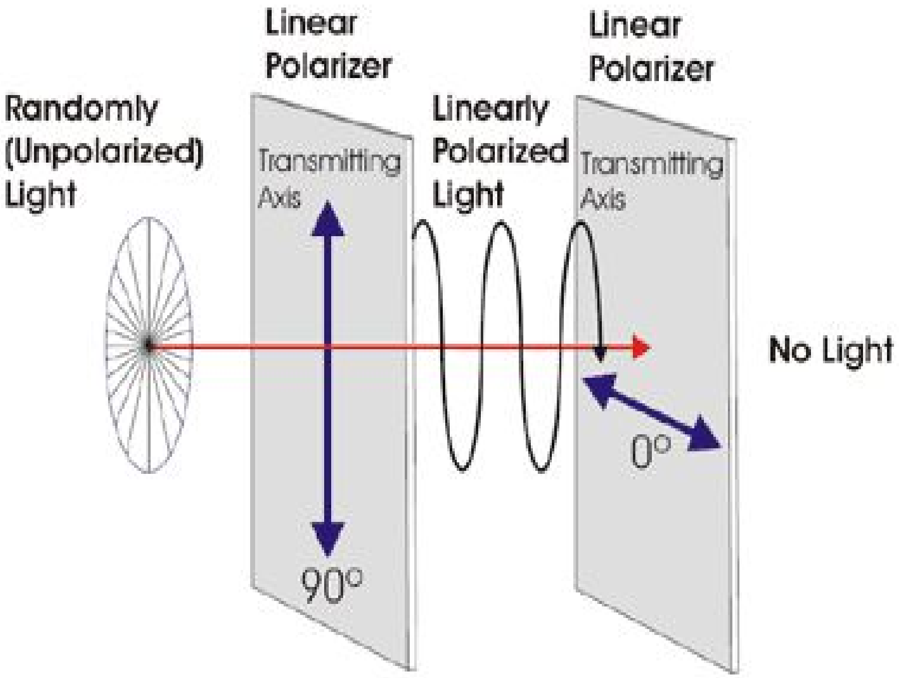
Let's try an experiment

3. Place the vertical filter after that



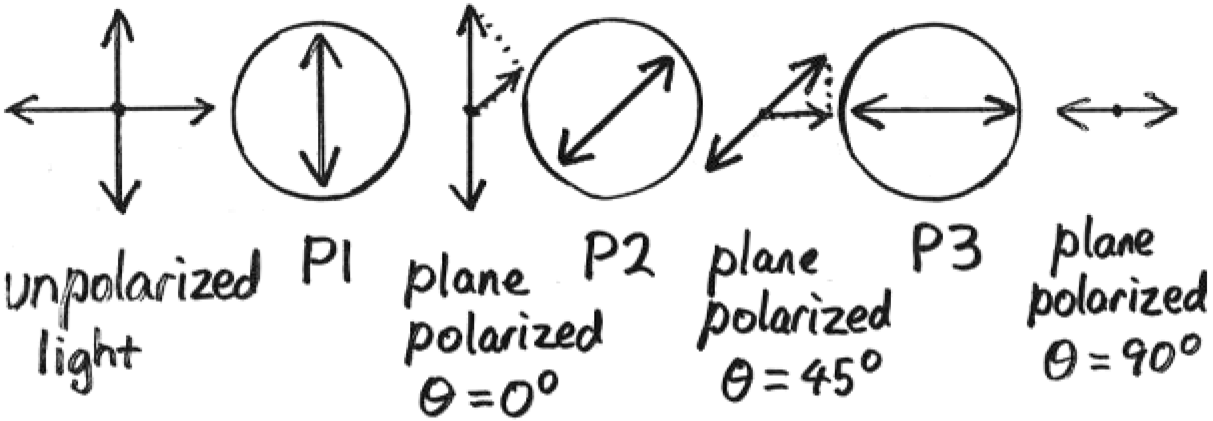
Let's try an experiment

3. Place the vertical filter after that → no light pass through it



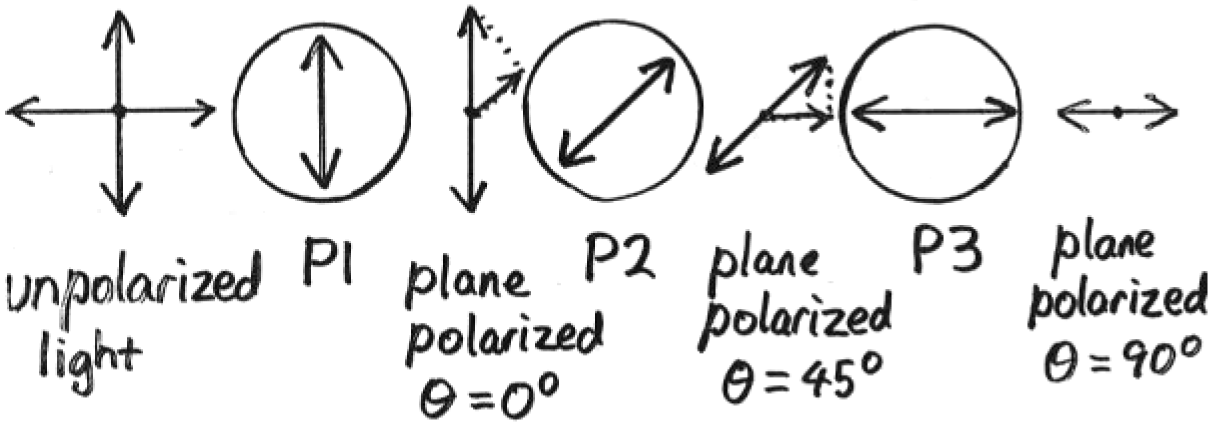
Let's try an experiment

4. Now place the 45° filter in between



Let's try an experiment

4. Now place the 45° filter in between → light starts to emerge from the vertical filter



Say waaaat?

- Think wavefunction & probabilities

Say waaaat?

- Think wavefunction & probabilities
- An arbitrary polarization can be represented by

$$|\psi\rangle = a_{\psi}|\uparrow\rangle + b_{\psi}|\downarrow\rangle$$

Say waaaat?

- Think wavefunction & probabilities
- An arbitrary polarization can be represented by

$$|\psi\rangle = a_\psi|\uparrow\rangle + b_\psi|\downarrow\rangle$$

- But we could change the basis:

$$|\uparrow\rangle = \frac{1}{\sqrt{2}}|\nwarrow\rangle + \frac{1}{\sqrt{2}}|\nearrow\rangle$$

Say waaaat?

- Think wavefunction & probabilities
- An arbitrary polarization can be represented by

$$|\psi\rangle = a_\psi|\uparrow\rangle + b_\psi|\downarrow\rangle$$

- But we could change the basis:

$$|\uparrow\rangle = \frac{1}{\sqrt{2}}|\nwarrow\rangle + \frac{1}{\sqrt{2}}|\nearrow\rangle$$

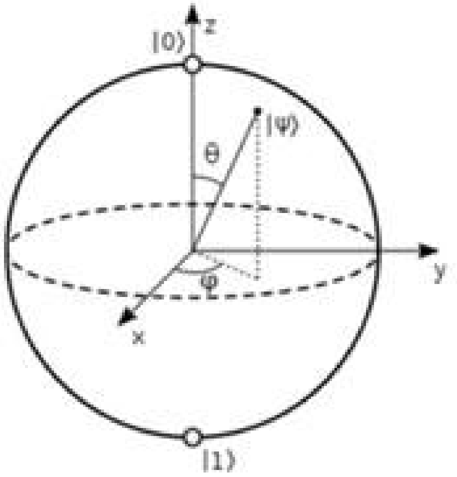
- Probability that the photon passes through: square of the amplitude, times 3

Enter Qubits [quantum bits]

Unit vector in a 2-dimensional complex vector space:

$$|\psi\rangle = A|0\rangle + B|1\rangle$$

$$|A|^2 + |B|^2 = 1$$



$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$\alpha = \cos\left(\frac{\theta}{2}\right)$$

$$\beta = e^{i\phi}\sin\left(\frac{\theta}{2}\right)$$

Enter several quibits

- 2 qubits

$$|\phi_1\rangle \otimes |\phi_2\rangle = a_1a_2|00\rangle + a_1b_2|01\rangle + a_2b_1|10\rangle + b_1b_2|11\rangle .$$

Enter several qubits

- 2 qubits

$$|\phi_1\rangle \otimes |\phi_2\rangle = a_1 a_2 |00\rangle + a_1 b_2 |01\rangle + a_2 b_1 |10\rangle + b_1 b_2 |11\rangle.$$

- 3 qubits

$$\begin{aligned}
P_+ \otimes I \otimes I &= \Big(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|\Big) \otimes \Big(|0\rangle\langle 0| + |1\rangle\langle 1|\Big) \otimes \Big(|0\rangle\langle 0| + |1\rangle\langle 1|\Big), \\
&= \frac{1}{2}\Big[|000\rangle\langle 000| + |001\rangle\langle 001| + |010\rangle\langle 010| + |011\rangle\langle 011| + \\
&+ |000\rangle\langle 100| + |001\rangle\langle 101| + |010\rangle\langle 110| + |011\rangle\langle 111| + \\
&+ |100\rangle\langle 000| + |101\rangle\langle 001| + |110\rangle\langle 010| + |111\rangle\langle 011| + \\
&+ |100\rangle\langle 100| + |101\rangle\langle 101| + |110\rangle\langle 110| + |111\rangle\langle 111|\Big],
\end{aligned}$$

http://astro.sunysb.edu/steinkirch/books/qi.pdf

Quantum mechanics give us spooky particles that can encode (and do) multiple things at once, just like a **massively parallel machine**

Shor's Algorithm

- PK crypto relies on a classical computer’s difficult at factoring large numbers (RSA, EC).

Shor's Algorithm

- PK crypto relies on a classical computer's difficult at factoring large numbers (RSA, EC).
- In 1994, Peter Shor showed that a QC could find the prime factors of a large number in milliseconds.

Shor's Algorithm

- PK crypto relies on a classical computer's difficult at factoring large numbers (RSA, EC).
- In 1994, Peter Shor showed that a QC could find the prime factors of a large number in milliseconds.
- In the moment when a QC is successfully built, **all the internet becomes insecure** (remember: no forward secrecy!)

Shor's Algorithm

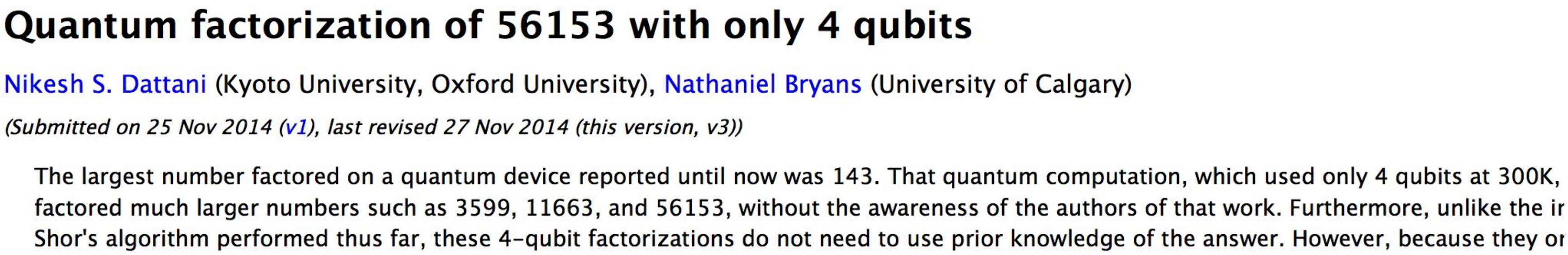
- For a 1000-bit number, all we need is ~1000 qubits (without error correction) for maybe just a dozen seconds

Shor's Algorithm

- For a 1000-bit number, all we need is ~1000 qubits (without error correction) for maybe just a dozen seconds
  - The wavefunction will encode 2**1000 possibilities (states)

Shor's Algorithm

- For a 1000-bit number, all we need is ~1000 qubits (without error correction) for maybe just a dozen seconds
  - The wavefunction will encode state 2**1000 possibilities



Quantum factorization of 56153 with only 4 qubits

Nikesh S. Dattani (Kyoto University, Oxford University), Nathaniel Bryans (University of Calgary)

(Submitted on 25 Nov 2014 (v1), last revised 27 Nov 2014 (this version, v3))

The largest number factored on a quantum device reported until now was 143. That quantum computation, which used only 4 qubits at 300K, factored much larger numbers such as 3599, 11663, and 56153, without the awareness of the authors of that work. Furthermore, unlike the ir Shor's algorithm performed thus far, these 4-qubit factorizations do not need to use prior knowledge of the answer. However, because they or

Shor's Algorithm: How?

- Quantum Fourier Transform to find the **periodicity of prime numbers**
- Algorithm runs simultaneously every pair of number: wavefunctions either constructly or desconstructly interfer
- In the end, the right answer spike (frequency/period/mod)

Alice & Bob are kinda scared now….

- But… what if Alice and Bob could use QM to create and distribute a key?

Alice & Bob are kinda scared now...

- But… what if Alice and Bob could use QM to create and distribute a key?

- Distribute qubits through a **quantum** channel to establish a key that can be used across a **classical** channel.

Alice, Bob and... Heisenberg

- QC security is based on the **Heisenberg Uncertainty principle**

$$\Delta p \, \Delta x \ \geq \frac{1}{2} \, \hbar$$

$$\Delta E \, \Delta t \ \geq \frac{1}{2} \, \hbar$$

Alice, Bob and... Heisenberg

- QC security is based on the **Heisenberg Uncertainty principle**
    - You **cannot make a perfect copy** of a quantum state without disturbing it, **introducing errors** in the communication.

$$\Delta p \, \Delta x \geq \frac{1}{2} \hbar$$

$$\Delta E \, \Delta t \geq \frac{1}{2} \hbar$$

not this...

Secure by ~~Math~~ Physics

- Alice and Bob can exchange (quantum encoded) keys securely (e.g. photons via fiber).

Secure by ~~Math~~ Physics

- Alice and Bob can exchange (quantum encoded) keys securely (e.g. photons via fiber).
- If Eve reads the state of photon → probability collapses and Bob and Alice will know!

Quantum Key Distribution (BB84)

1. Alice prepares a sequence of photons, polarize each one in of the four possibilities of polarization.

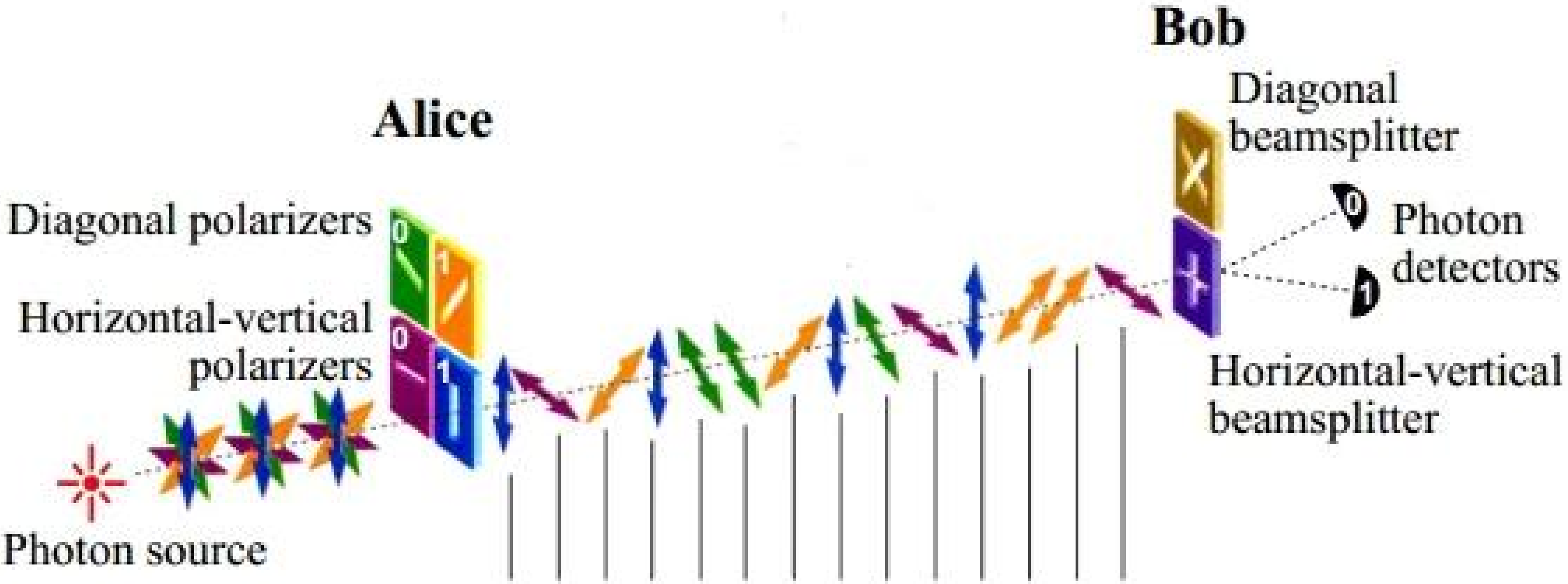
Quantum Key Distribution [BB84]

1. Alice prepares a sequence of photons, polarize each one in of the four possibilities of polarization.
2. Bob measures these photons in the 2 basis, and keep bits values in secret.

Quantum Key Distribution [BB84]

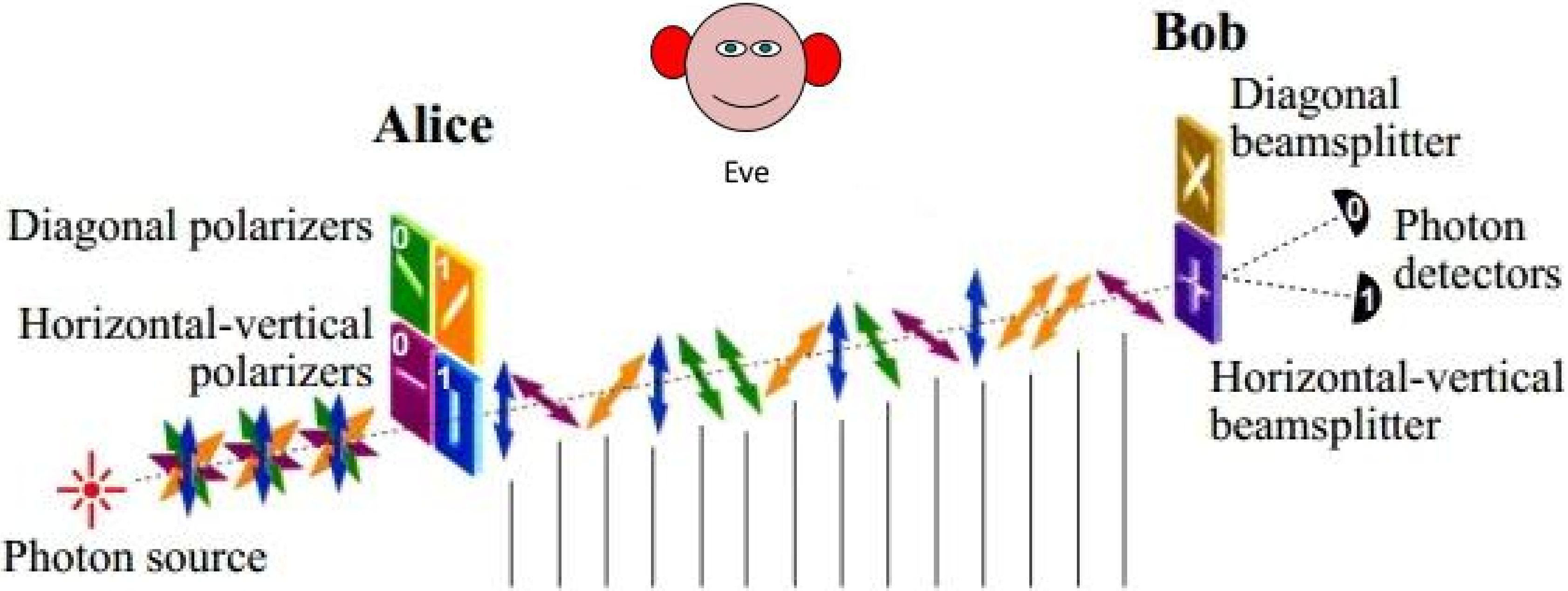
1. Alice prepares a sequence of photons, polarize each one in of the four possibilities of polarization.
2. Bob measures these photons in random basis, and take note of the bits values.
3. Alice and Bob compare their basis but not the bit values, discarding the wrong measurements.

Quantum Key Distribution (BB84)



Alice's bit sequence	1	0	1	1	0	0	1	1	0	0	1	1	1	0	
	+	×	+	+	×	×	+	+	×	+	×	×	+	+	Bob's detection basis
	1	0	0	1	0	0	1	1	0	0	0	1	0	0	Bob's measurement
Sifted key	1	–	–	1	0	0	–	1	0	0	–	1	–	0	Sifted key

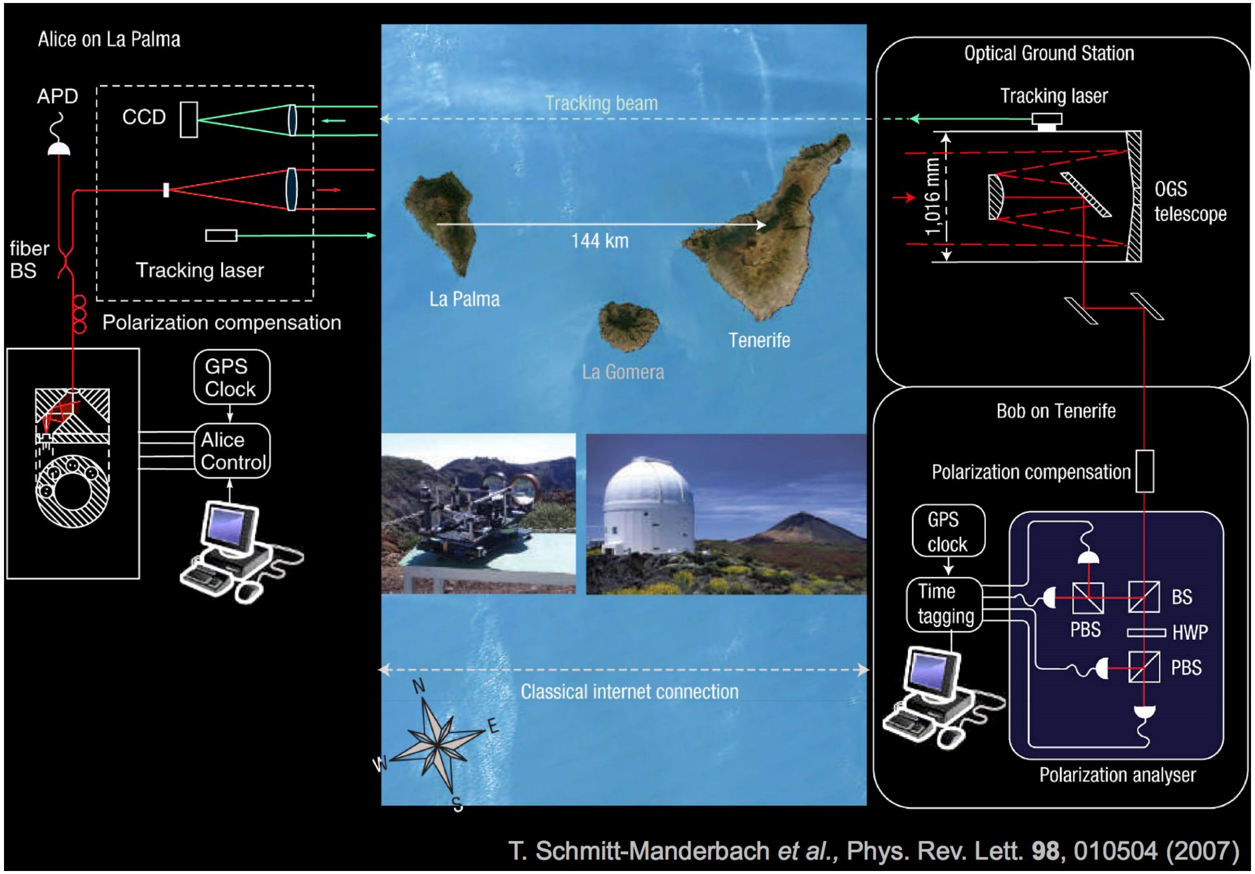
Quantum Key Distribution (BB84)



Alice's bit sequence	1	0	1	1	0	0	1	1	0	0	1	1	1	0	
	+	×	+	+	×	×	+	+	×	+	×	×	+	+	Bob's detection basis
	1	0	0	1	0	0	1	1	0	0	0	1	0	0	Bob's measurement
Sifted key	1	–	–	1	0	0	–	1	0	0	–	1	–	0	Sifted key

Free-space QKD over 90 miles

Canary Islands: single photons prepared in La Palma and sent to Tenerife



T. Schmitt-Manderbach *et al.*, Phys. Rev. Lett. **98**, 010504 (2007)

All this is super cool... But how long is going to take for the first quantum computer?

Challenges in building a QC

- QCs must maintain hundreds of qubits together for some amount of time

Challenges in building a QC

- QCs must maintain hundreds of qubits together for some amount of time
  - **Decoherence:** The universe is observing all the time!
  - Particles are absorbed by the room and vanished!

But progress is happening

Particle control in a quantum world

***Serge Haroche** and **David J. Wineland** have independently invented and developed ground-breaking methods for measuring and manipulating individual particles while preserving their quantum-mechanical nature, in ways that were previously thought unattainable.*

The Nobel Prize in Physics 2012

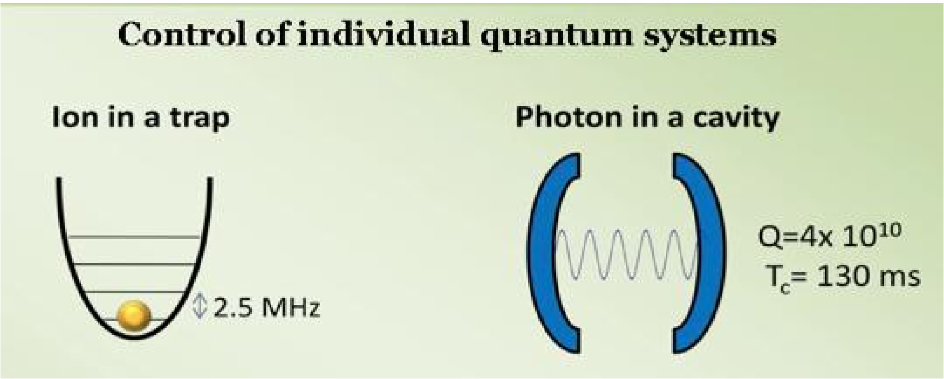


Photo: U. Montan

Serge Haroche

Prize share: 1/2

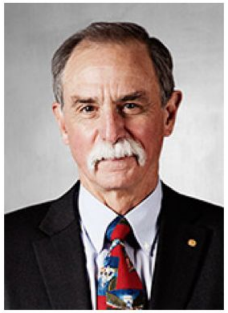


Photo: U. Montan

David J. Wineland

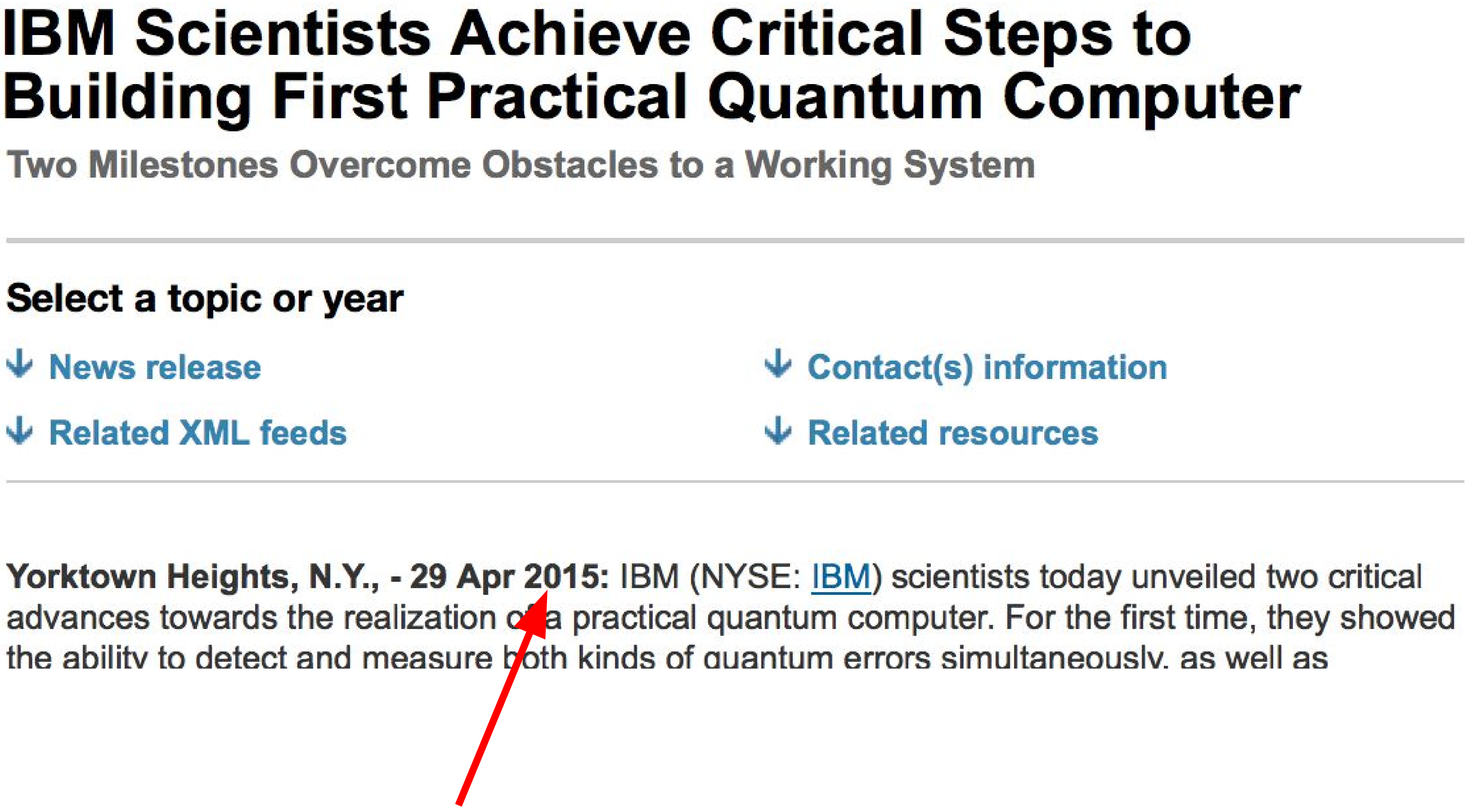
Prize share: 1/2

The Nobel Prize in Physics 2012 was awarded jointly to Serge Haroche and David J. Wineland *"for ground-breaking experimental methods that enable measuring and manipulation of individual quantum systems"*

Just 2-state quantum systems...

- Superconductor-based quantum computers (SQUIDs)
- Trapped ion quantum computer
- Optical lattices
- Topological quantum computer
- Quantum dot on surface (e.g. Loss-DiVincenzo)
- Nuclear magnetic resonance
- Cavity quantum electrodynamics (CQED)
- ...

Progress is happening



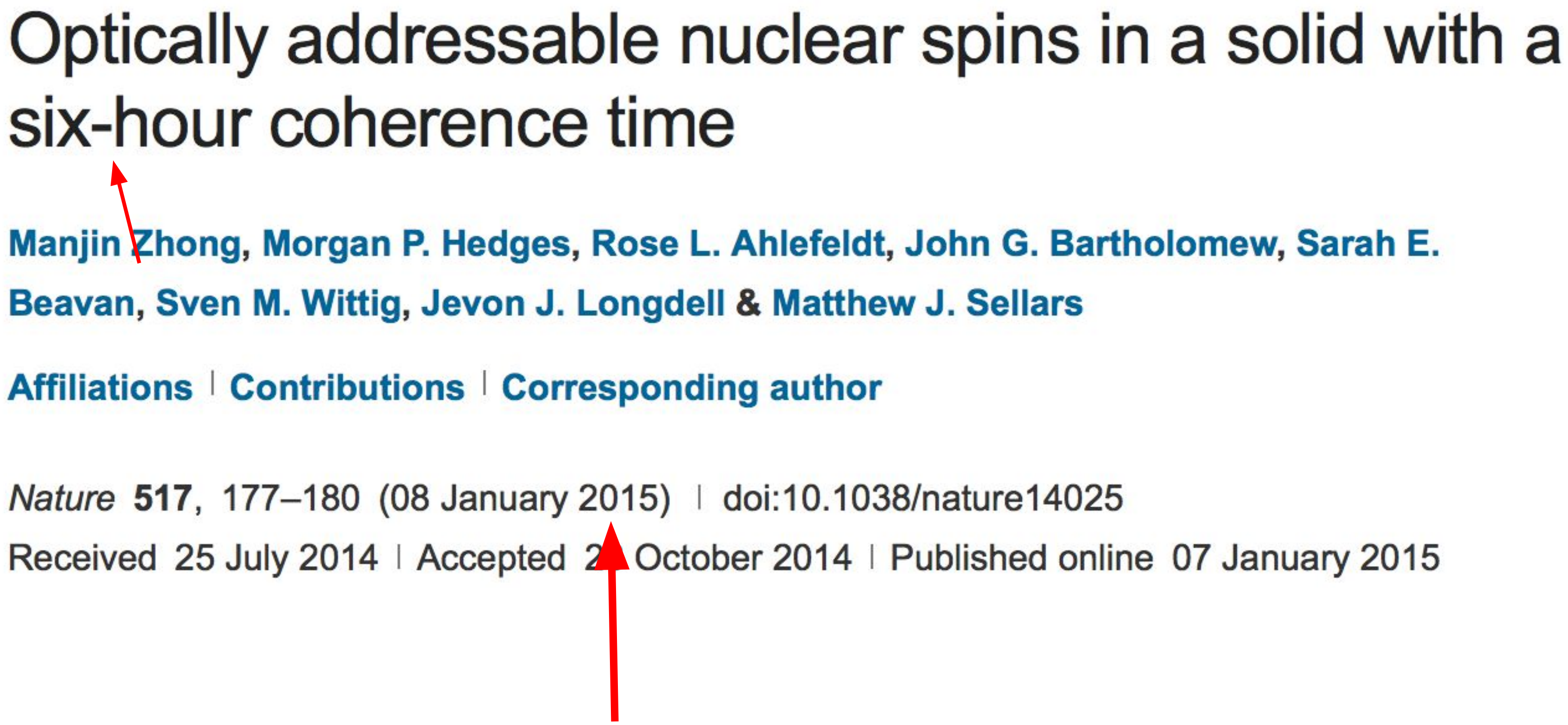
IBM Scientists Achieve Critical Steps to Building First Practical Quantum Computer

Two Milestones Overcome Obstacles to a Working System

Select a topic or year

Yorktown Heights, N.Y., - 29 Apr 2015: IBM (NYSE: IBM) scientists today unveiled two critical advances towards the realization of a practical quantum computer. For the first time, they showed the ability to detect and measure both kinds of quantum errors simultaneously, as well as

Progress is happening



Optically addressable nuclear spins in a solid with a six-hour coherence time

Manjin Zhong, Morgan P. Hedges, Rose L. Ahlefeldt, John G. Bartholomew, Sarah E. Beavan, Sven M. Wittig, Jevon J. Longdell & Matthew J. Sellars

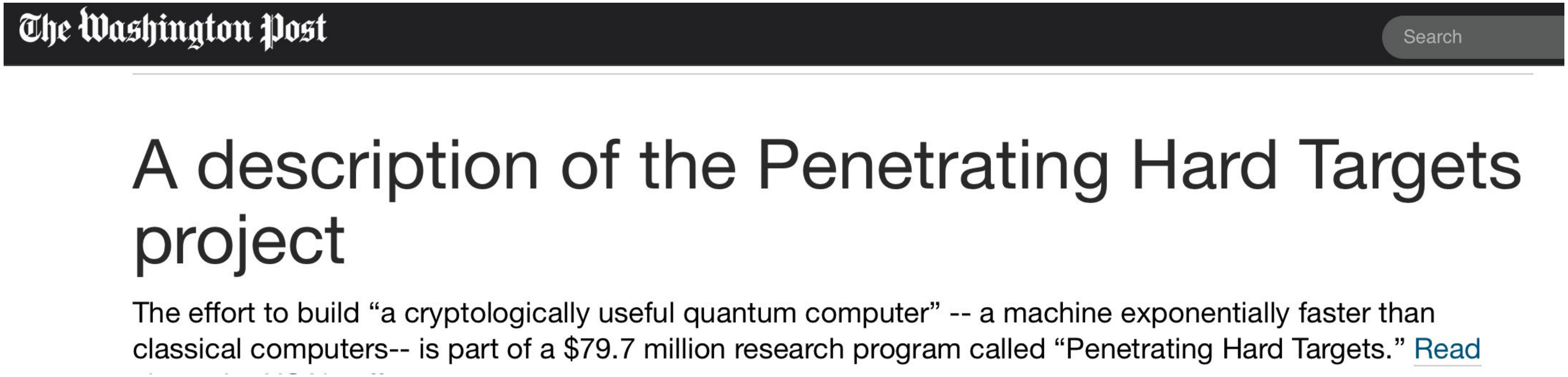
Affiliations | Contributions | Corresponding author

Nature **517**, 177–180 (08 January 2015) | doi:10.1038/nature14025

Received 25 July 2014 | Accepted 2[illegible] October 2014 | Published online 07 January 2015

For good or for bad

Snowden: **NSA** seeks to build quantum computer with a **$79.7 million research** program (jan/2014)



A description of the Penetrating Hard Targets project

The effort to build “a cryptologically useful quantum computer” -- a machine exponentially faster than classical computers-- is part of a $79.7 million research program called “Penetrating Hard Targets.” Read

Final Remarks

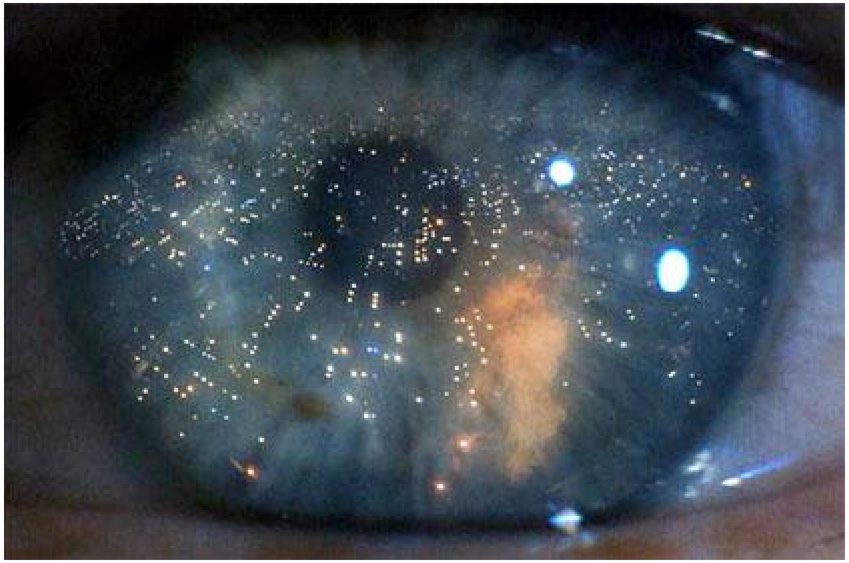
- There are lots more:
  - quantum algorithms (Grover, Simons), quantum gates/circuits, topological quantum computing, Deutsch parallelism, entanglement, quantum teleportation...

Final Remarks

- There are lots more:
  - quantum algorithms (Grover, Simons), quantum gates/circuits, topological quantum computing, Deutsch parallelism, Entanglement, quantum teleportation...

- This is a background, now you decide.

It's a brave new world...



Thank you.