Title: Introduction to quantum technologies: quantum computers, quantum teleporters & quantum cryptography

Date: May 27, 2006 09:00 AM

URL: http://pirsa.org/06050018

Abstract: <kw> Quantum cryptography, quantum physics, cryptography, one-time pad, RSA, encryption, public key, decryption, private key, quantum computer, qubit, quantum key, distribution, QKD, Moore\'s Law, probability, quantum theory, complex number, beam splitter, superposition, electron orbital, Turing, quantum parallelism, EPR, Bell, information security </kw>

University of Waterloo

PERIMETER INSTITUTE
FOR THEORETICAL PHYSICS

IQC Institute for Quantum Computing

Introduction to quantum technologies: quantum computers, quantum teleporters & cryptography

Michele Mosca

Canada Research Chair in Quantum Computation

OAPT

27 May 2006

Physics and Computation

Physics and Computation

- Information is stored in a physical medium, and manipulated by physical processes.

Physics and Computation

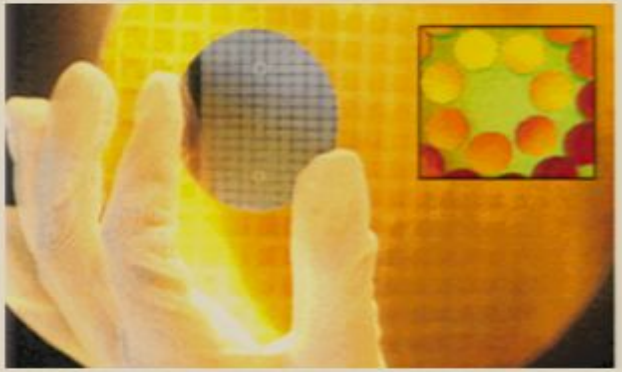
- Information is stored in a physical medium, and manipulated by physical processes.
- The laws of physics dictate the capabilities of any information processing device.

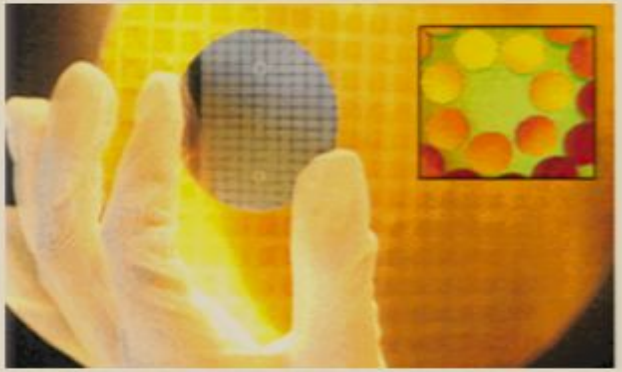
Physics and Computation

- Information is stored in a physical medium, and manipulated by physical processes.
- The laws of physics dictate the capabilities of any information processing device.
- Designs of "classical" computers are implicitly based in the *classical* framework for physics

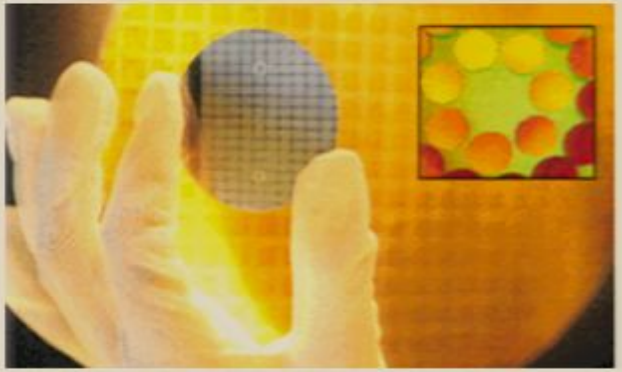
Physics and Computation

- Information is stored in a physical medium, and manipulated by physical processes.
- The laws of physics dictate the capabilities of any information processing device.
- Designs of "classical" computers are implicitly based in the *classical* framework for physics
- Classical physics is known to be wrong or incomplete… and has been replaced by a more powerful framework: *quantum mechanics*.



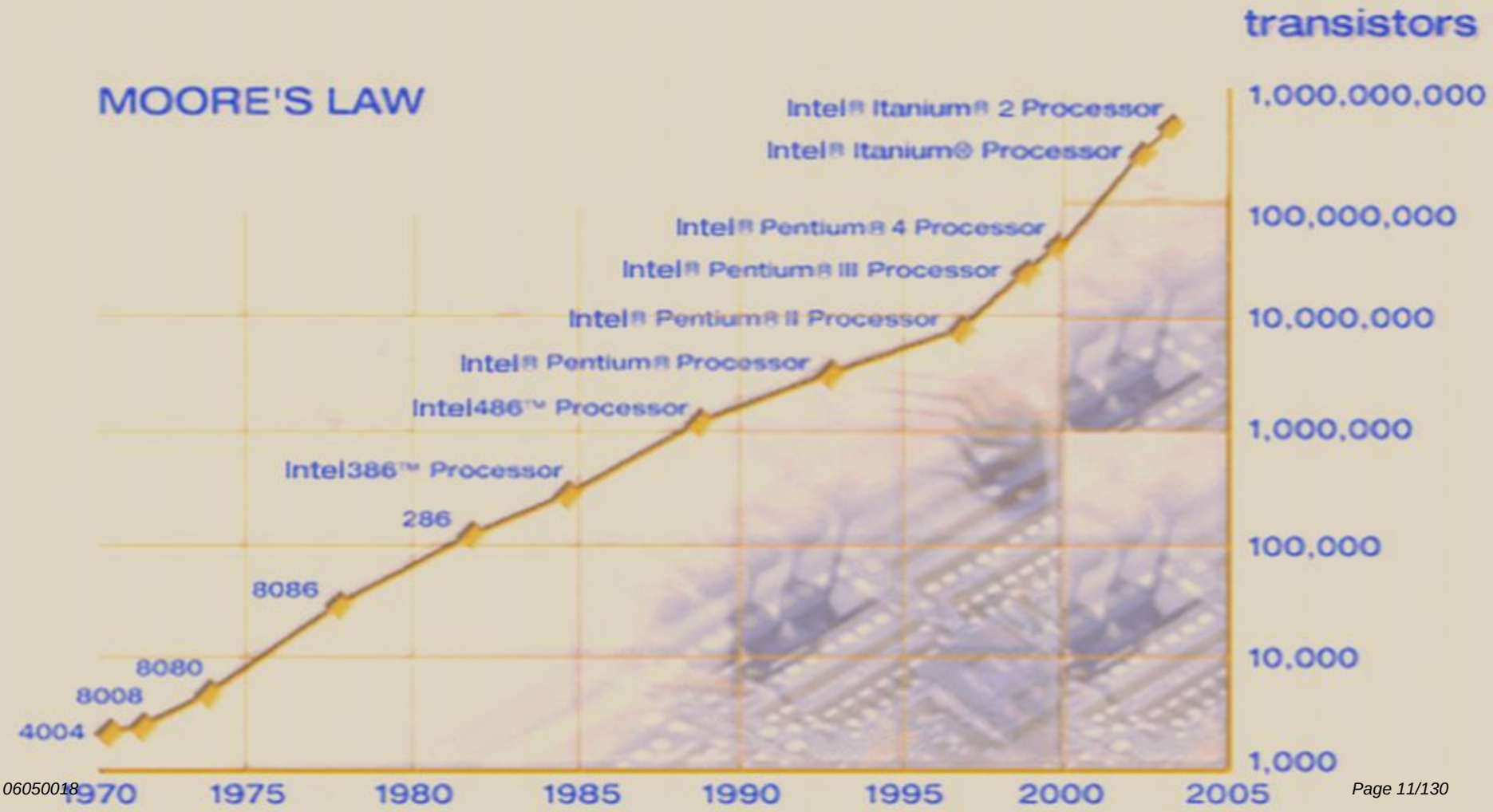


Computer technology is making devices smaller and smaller…



Computer technology is making devices smaller and smaller…

…reaching a point where classical physics is no longer a suitable model for the laws of physics.


MOORE'S LAW
transistors
Intel® Itanium® 2 Processor
Intel® Itanium® Processor
Intel® Pentium® 4 Processor
Intel® Pentium® III Processor
Intel® Pentium® II Processor
Intel® Pentium® Processor
Intel486™ Processor
Intel386™ Processor
286
8086
8080
8008
4004
1,000,000,000
100,000,000
10,000,000
1,000,000
100,000
10,000
1,000
1970
1975
1980
1985
1990
1995
2000
2005

The design of devices on such a small scale will *require* engineers to control quantum mechanical effects.

The design of devices on such a small scale will *require* engineers to control quantum mechanical effects.

Allowing computers to take advantage of quantum mechanical behaviour allows us to do *more* than cram increasingly many microscopic components onto a silicon chip…

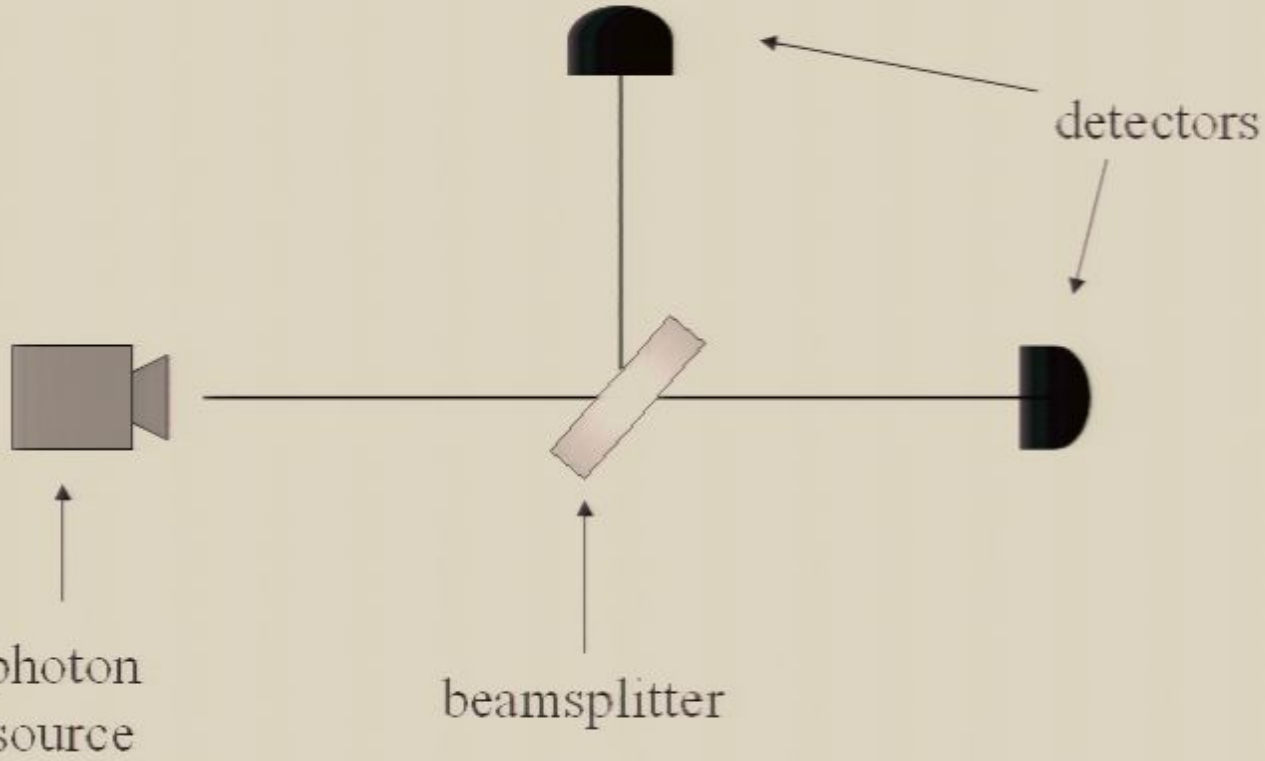
The design of devices on such a small scale will *require* engineers to control quantum mechanical effects.

Allowing computers to take advantage of quantum mechanical behaviour allows us to do *more* than cram increasingly many microscopic components onto a silicon chip…

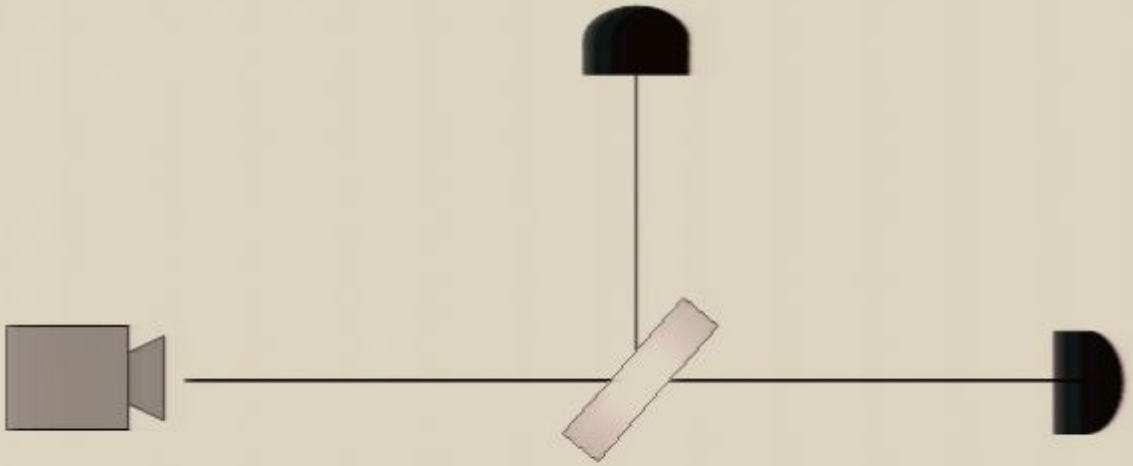
… it gives us a whole new framework in which information can be processed in *fundamentally new ways*.

A simple experiment in optics

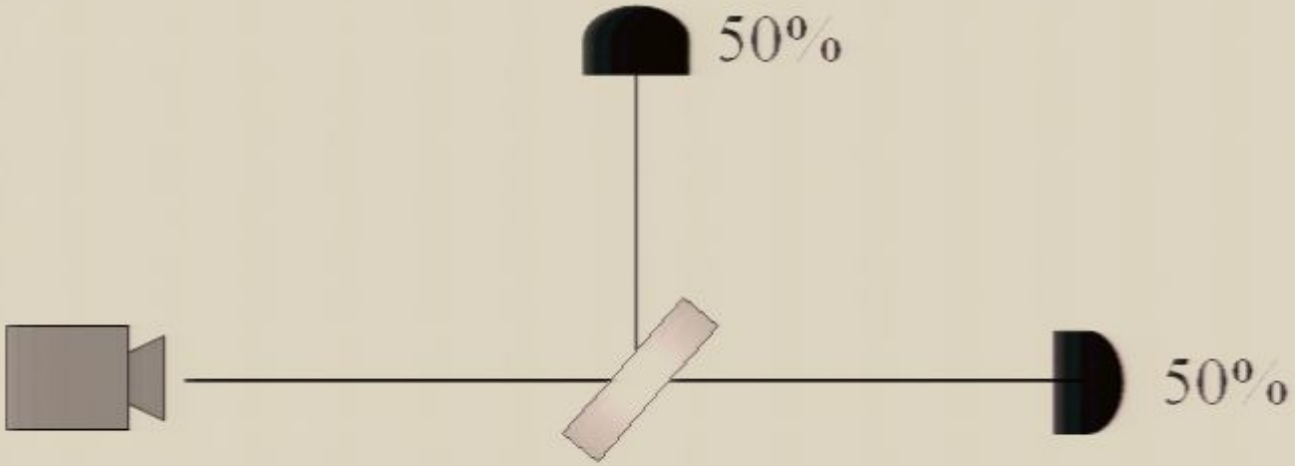
...consider a setup involving a photon source, a half-silvered mirror (beamsplitter), and a pair of photon detectors.



Now consider what happens when we fire a single photon into the device…



Now consider what happens when we fire a single photon into the device…

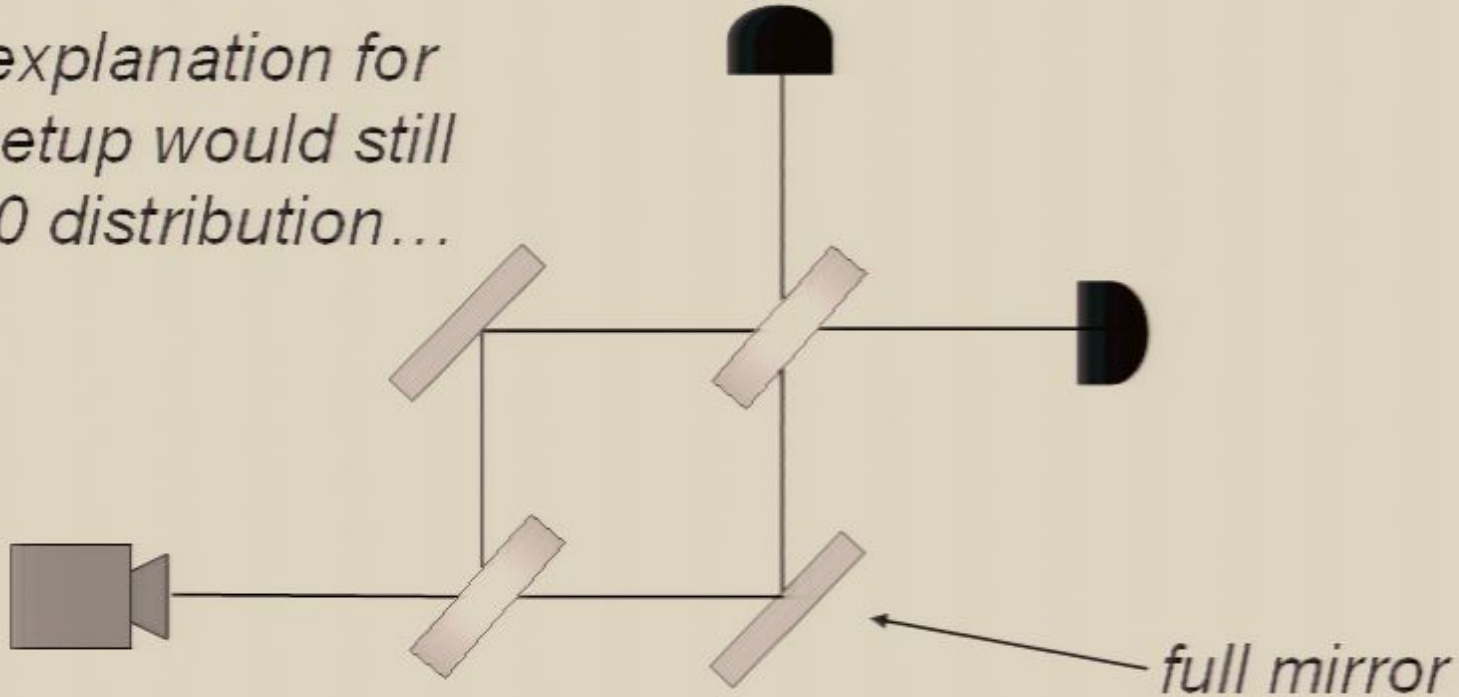


Simplest explanation: beam-splitter acts as a classical coin-flip, randomly sending each photon one way or the other.

The "weirdness" of quantum mechanics…

… consider a modification of the experiment…

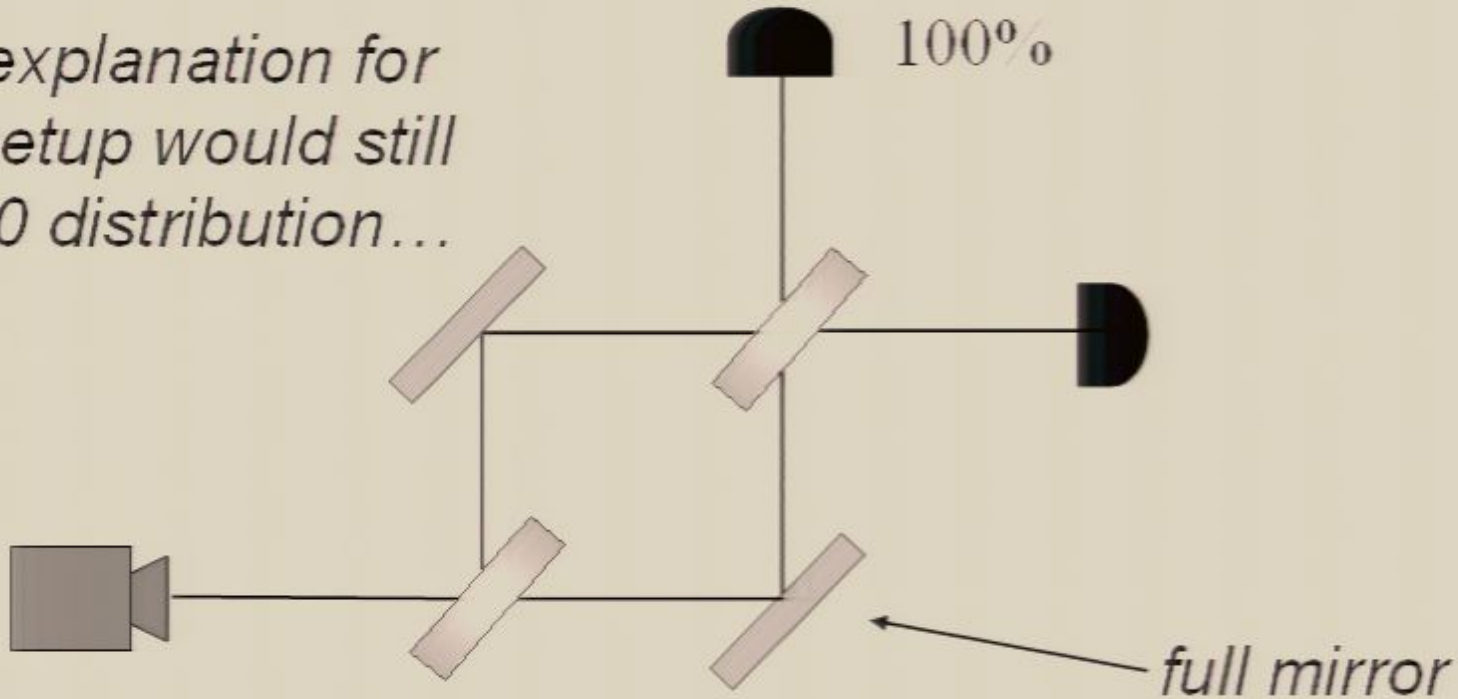
The simplest explanation for the modified setup would still predict a 50-50 distribution…



The "weirdness" of quantum mechanics…

… consider a modification of the experiment…

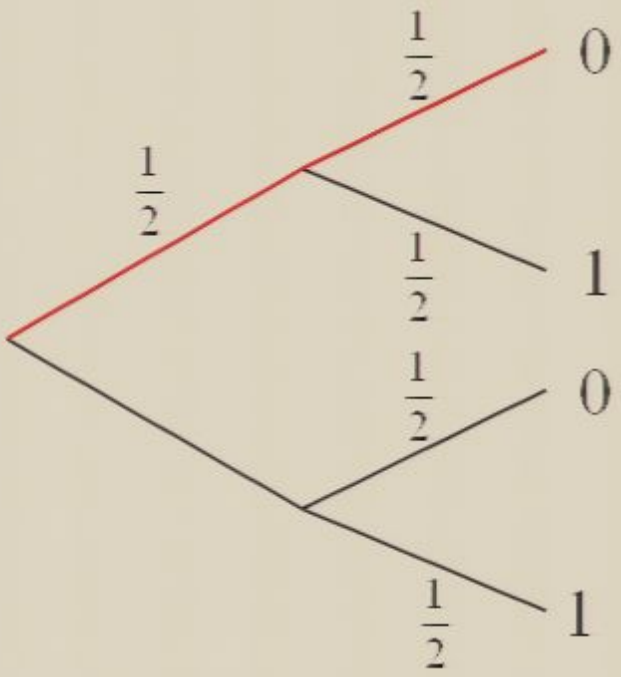
The simplest explanation for the modified setup would still predict a 50-50 distribution…



The simplest explanation is wrong!

Classical probabilities…

Consider a computation tree for a simple two-step (classical) probabilistic algorithm, which makes a coin-flip at each step, and whose output is 0 or 1:



The probability of the computation following a given path is obtained by multiplying the probabilities along all branches of that path… in the example the probability the computation follows the red path is

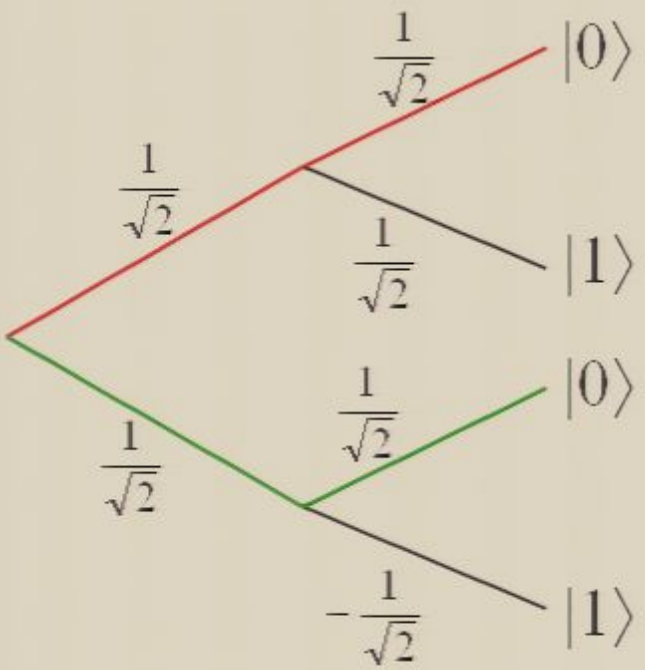
$$\frac{1}{2}\cdot\frac{1}{2}=\frac{1}{4}$$

The probability of the computation giving the answer 0 is obtained by adding the probabilities of all paths resulting in 0:

$$\frac{1}{4}+\frac{1}{4}=\frac{1}{2}$$

...vs quantum probabilities ...

In quantum physics, we have probability *amplitudes*, which can have complex phase factors associated with them.



The probability *amplitude* associated with a path in the computation tree is obtained by multiplying the probability *amplitudes* on that path. In the example, the red path has amplitude 1/2, and the green path has amplitude –1/2.

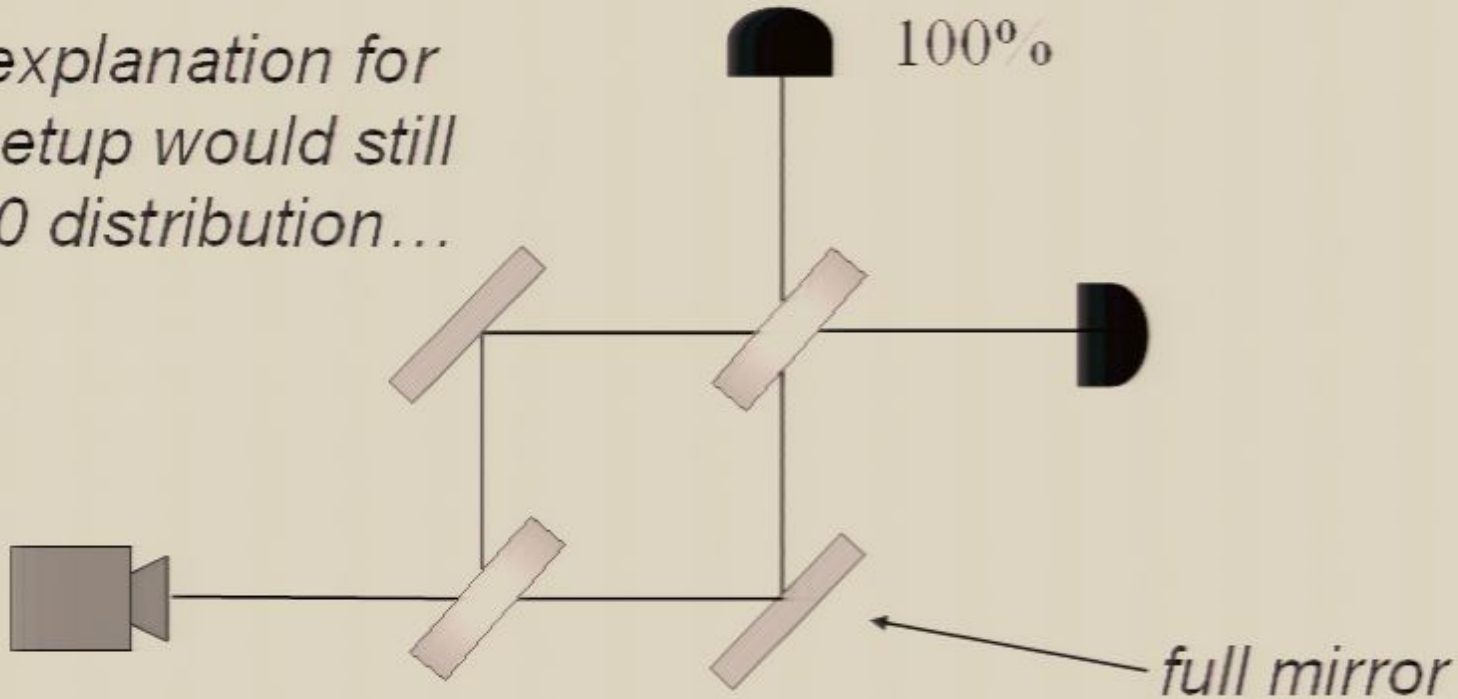
The probability amplitude for getting the answer $|1\rangle$ is obtained by adding the probability amplitudes... notice that the phase factors can lead to cancellations! The probability of obtaining $|1\rangle$ is obtained by squaring the total probability amplitude. In the example the probability of getting $|1\rangle$ is

$$\left(\frac{1}{2}-\frac{1}{2}\right)^2 = 0$$

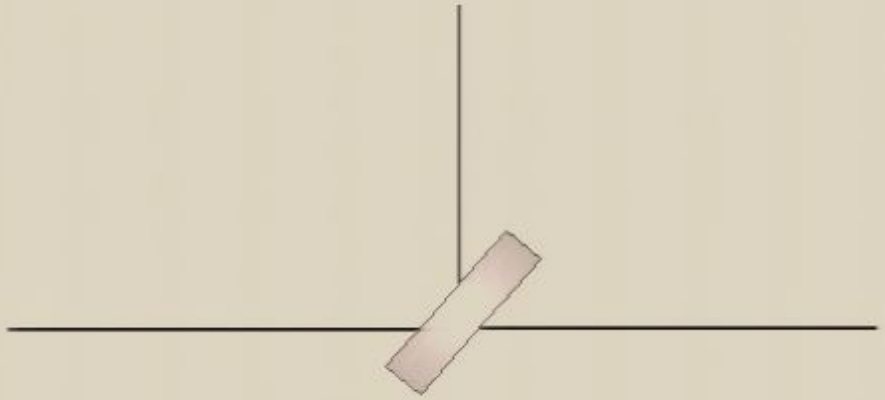
The "weirdness" of quantum mechanics…

… consider a modification of the experiment…

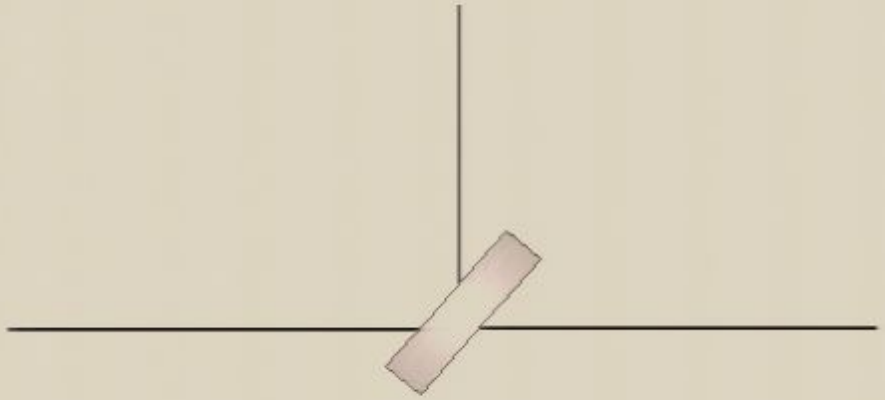
The simplest explanation for the modified setup would still predict a 50-50 distribution…



Beamsplitter described by quantum probability rules…



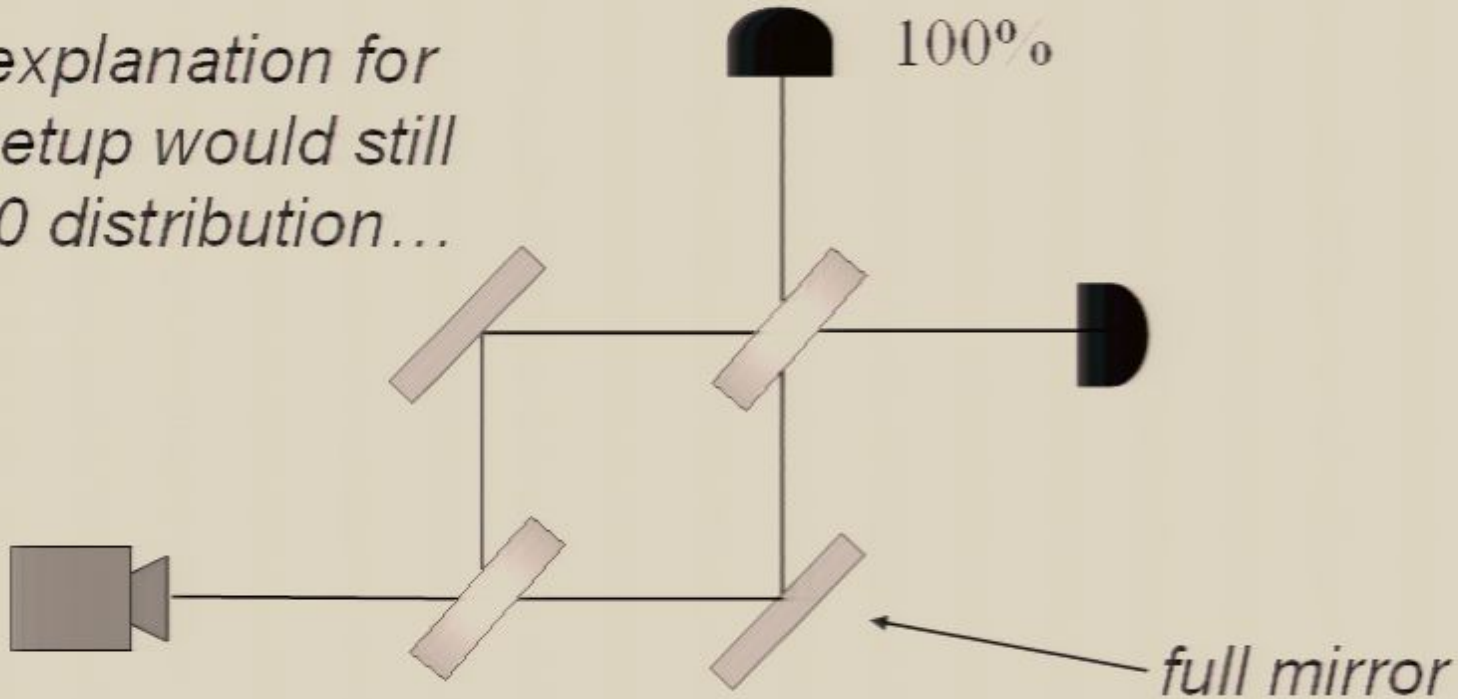
Beamsplitter described by quantum probability rules…



The "weirdness" of quantum mechanics…

… consider a modification of the experiment…

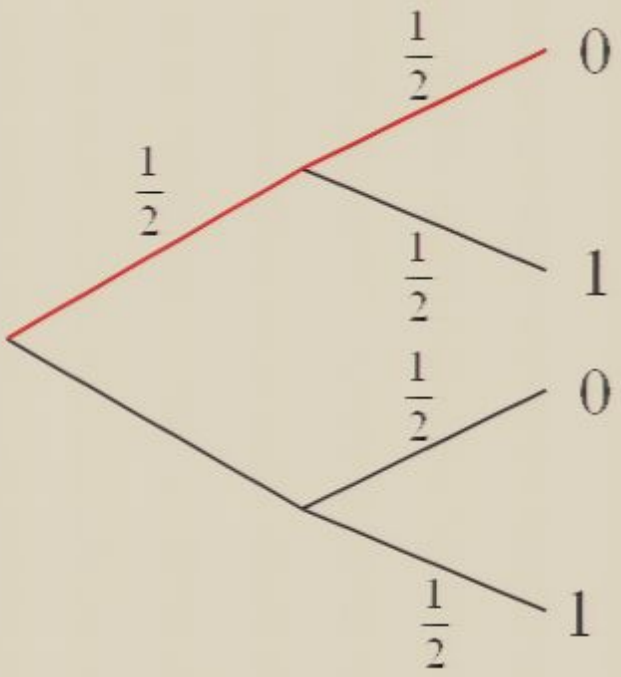
The simplest explanation for the modified setup would still predict a 50-50 distribution…



The simplest explanation is wrong!

Classical probabilities…

Consider a computation tree for a simple two-step (classical) probabilistic algorithm, which makes a coin-flip at each step, and whose output is 0 or 1:



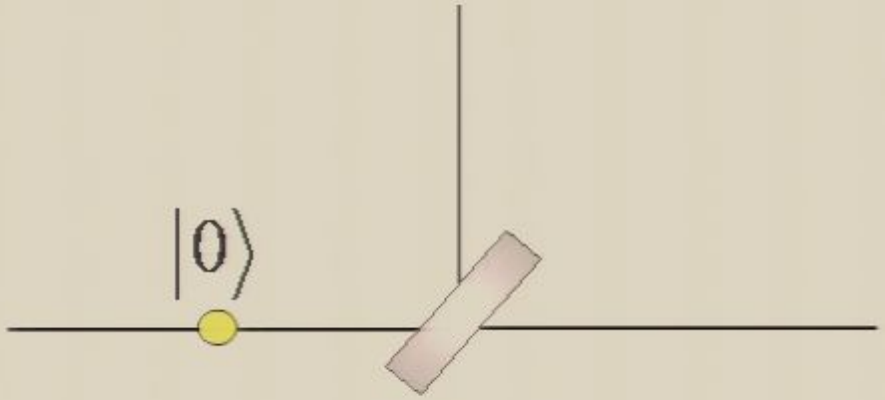
The probability of the computation following a given path is obtained by multiplying the probabilities along all branches of that path… in the example the probability the computation follows the red path is

$$\frac{1}{2}\cdot\frac{1}{2}=\frac{1}{4}$$

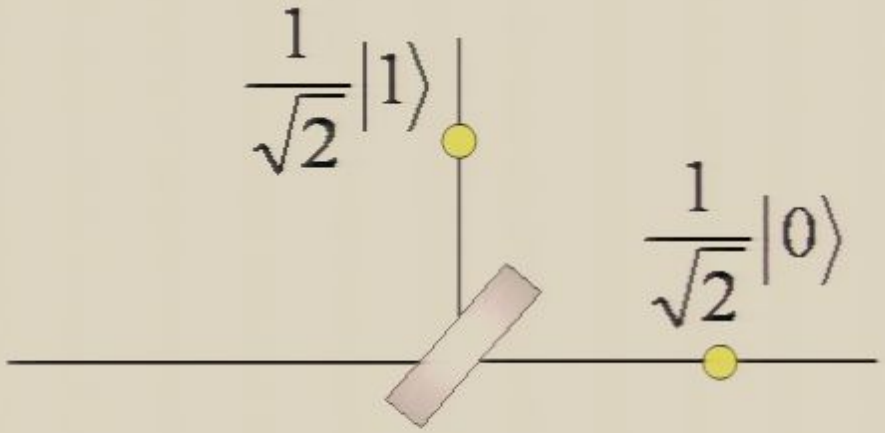
The probability of the computation giving the answer 0 is obtained by adding the probabilities of all paths resulting in 0:

$$\frac{1}{4}+\frac{1}{4}=\frac{1}{2}$$

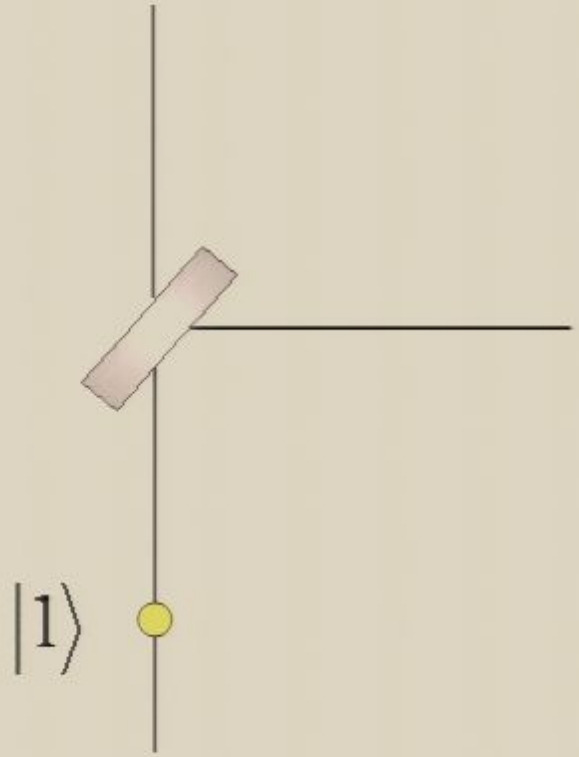
Beamsplitter described by quantum probability rules…



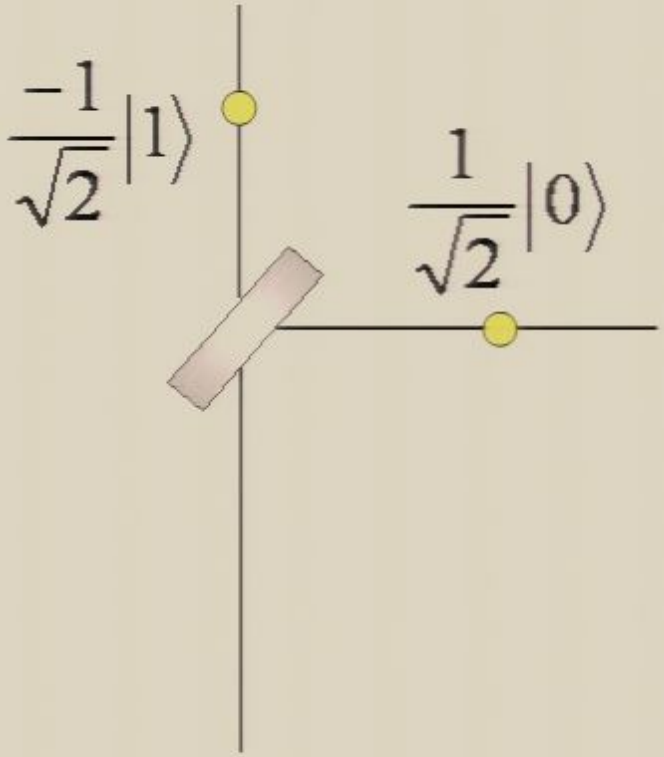
Beamsplitter described by quantum probability rules…



Beamsplitter described by quantum probability rules…



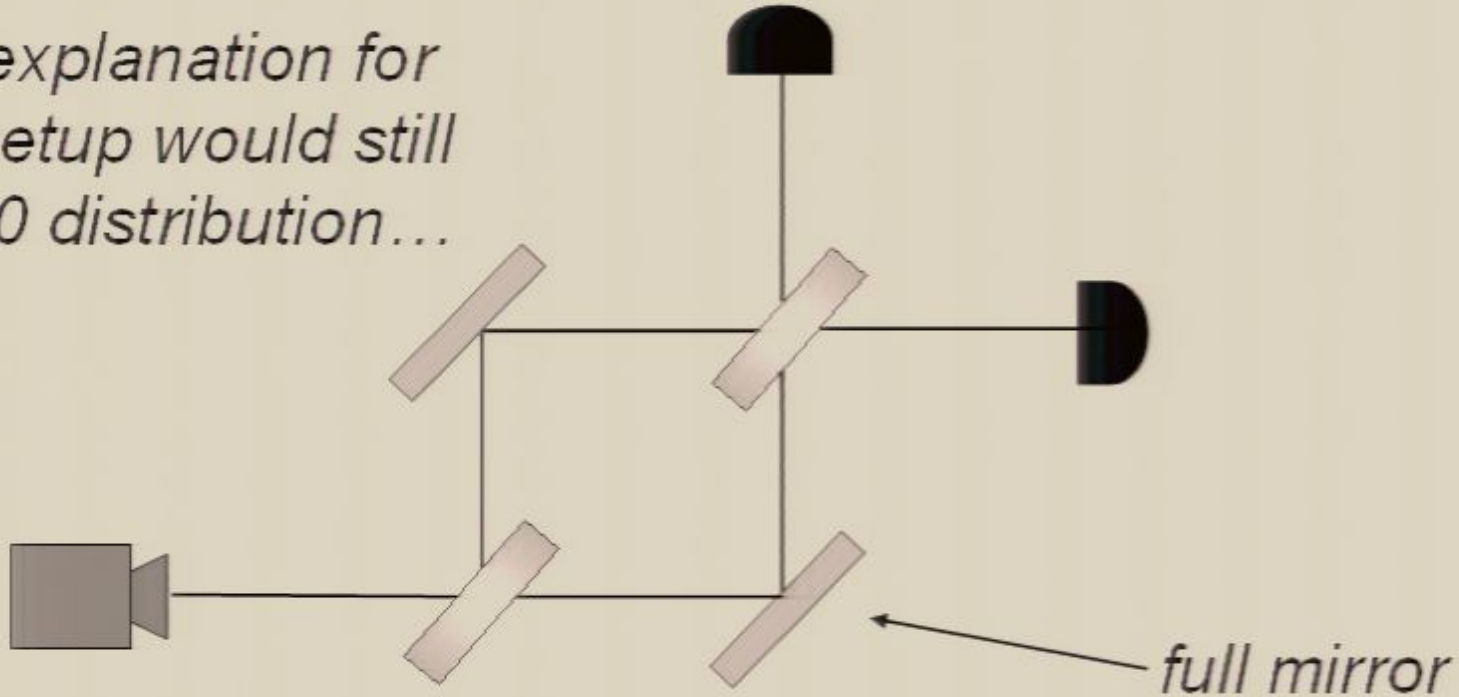
Beamsplitter described by quantum probability rules…



Explanation of experiment

… consider a modification of the experiment…

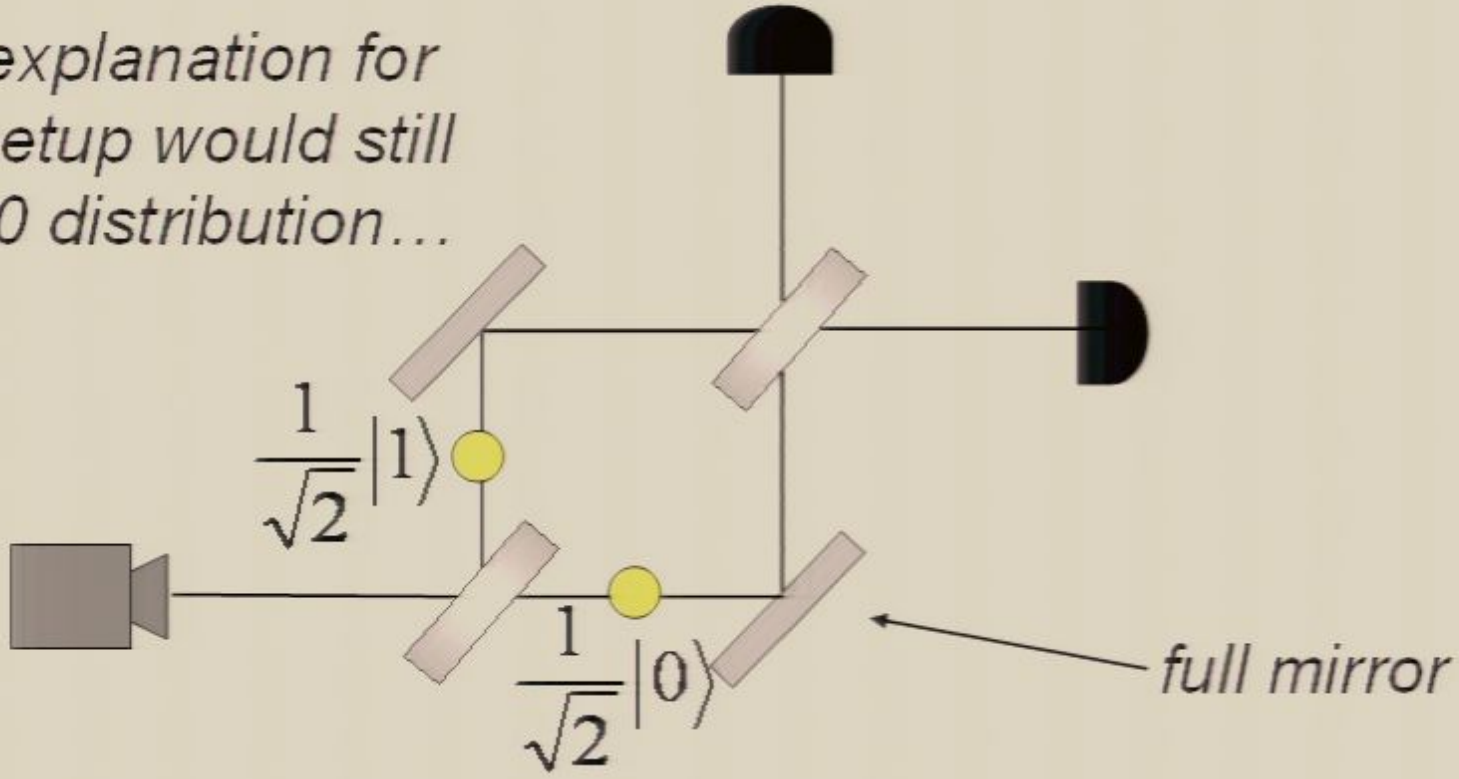
The simplest explanation for the modified setup would still predict a 50-50 distribution…



Explanation of experiment

… consider a modification of the experiment…

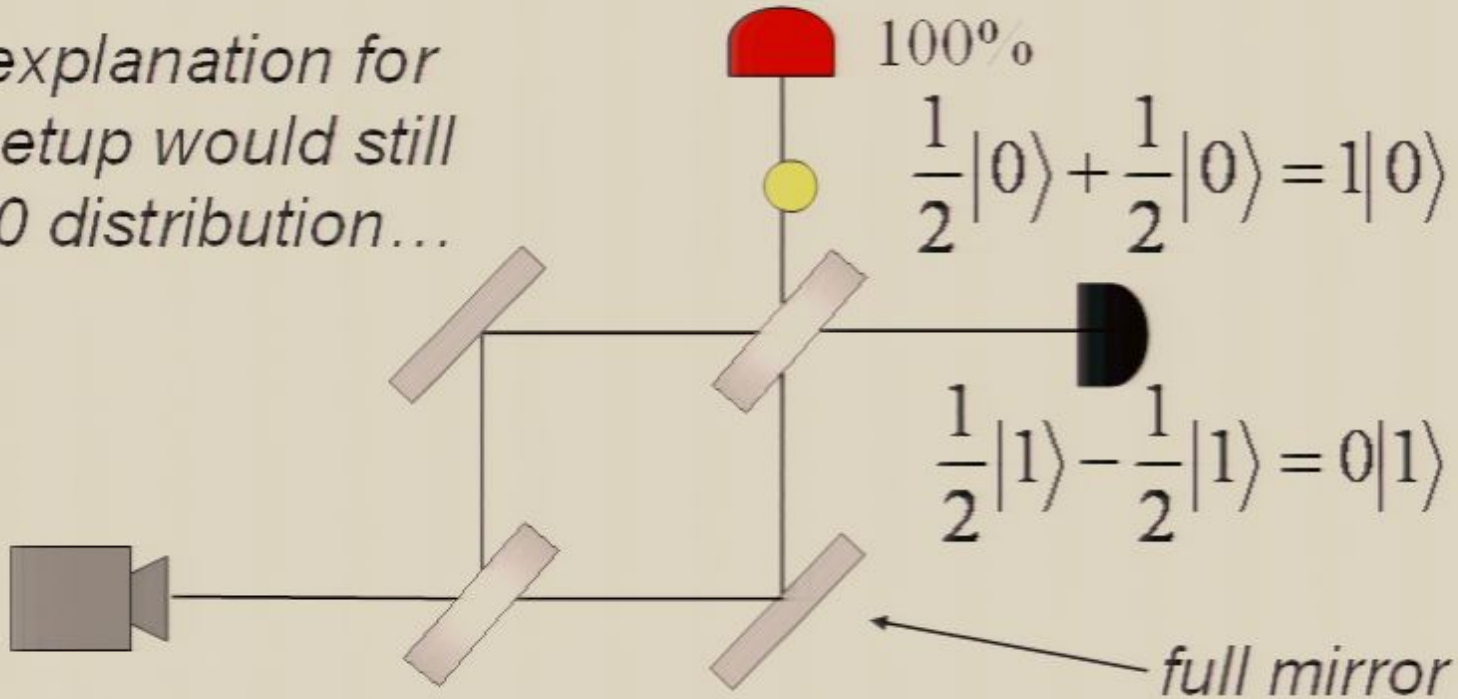
The simplest explanation for the modified setup would still predict a 50-50 distribution…



Explanation of experiment

… consider a modification of the experiment…

The simplest explanation for the modified setup would still predict a 50-50 distribution…



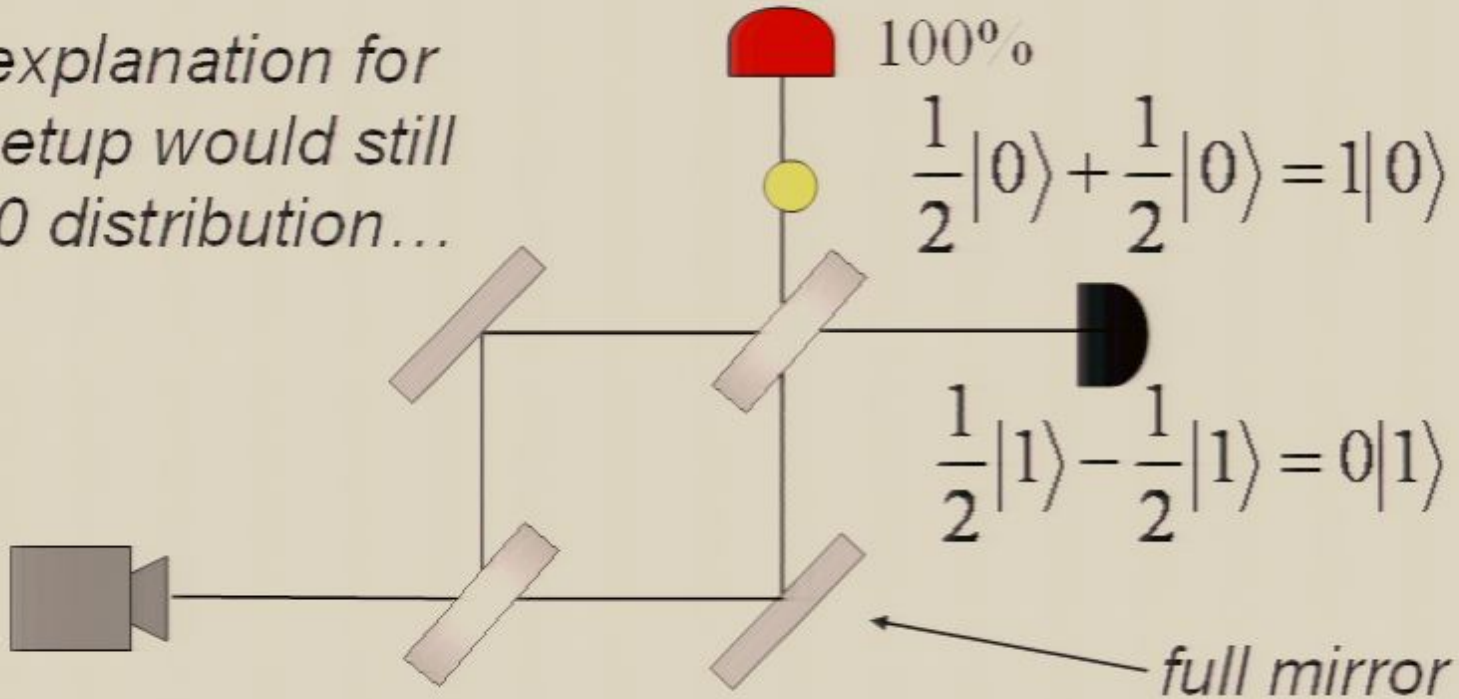
Another physical example

$|0\rangle$

Explanation of experiment

… consider a modification of the experiment…

The simplest explanation for the modified setup would still predict a 50-50 distribution…



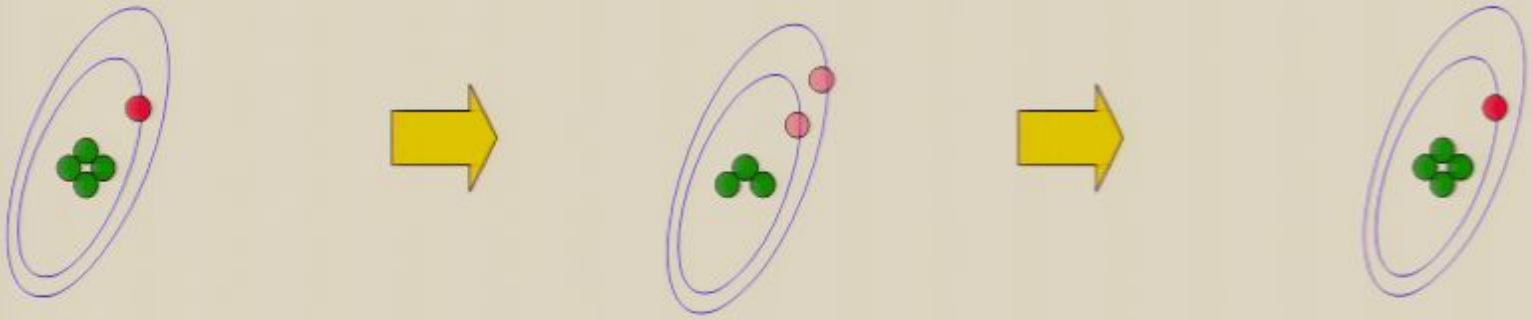
Another physical example

$|0\rangle$

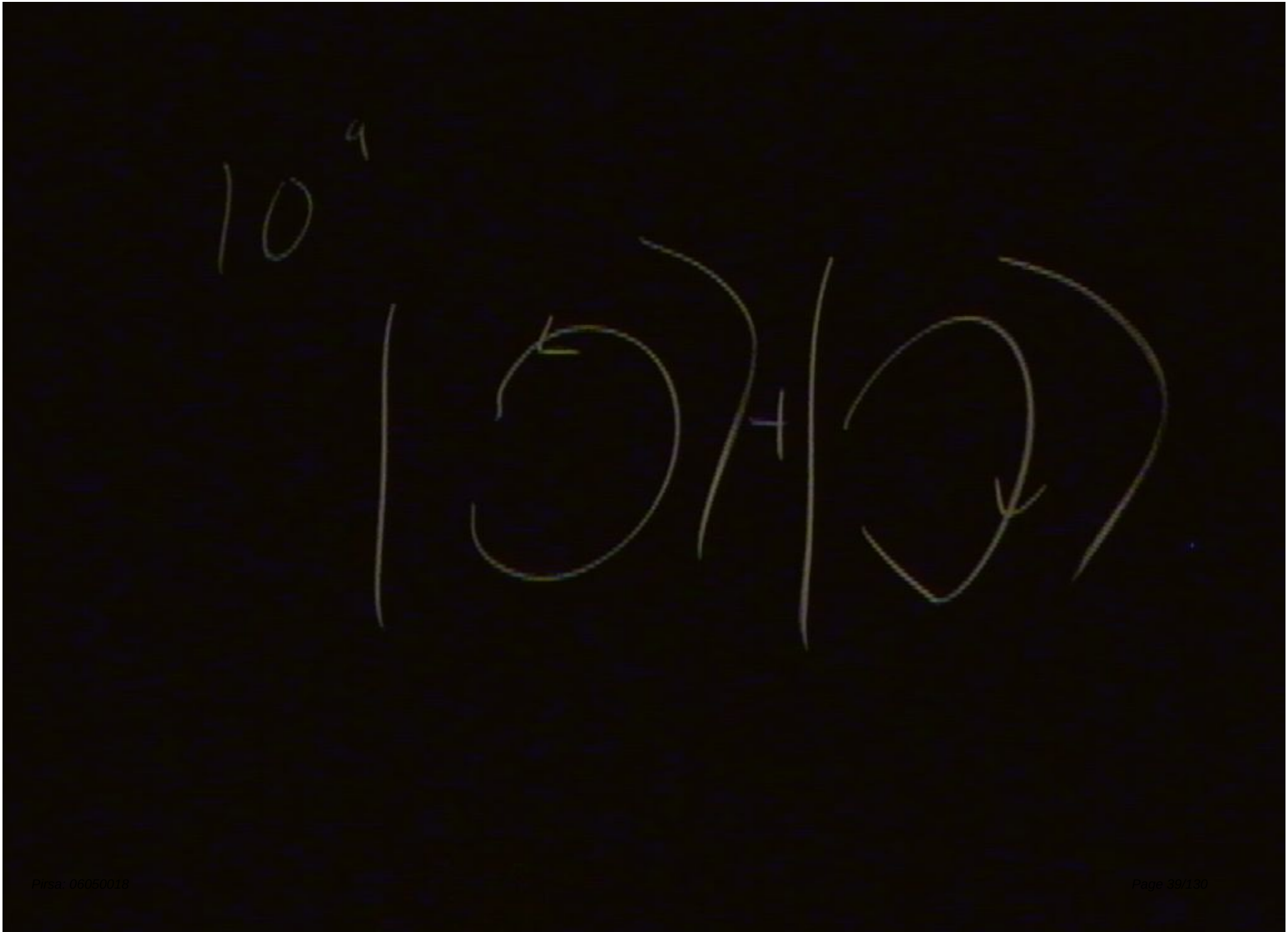
Another physical example

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

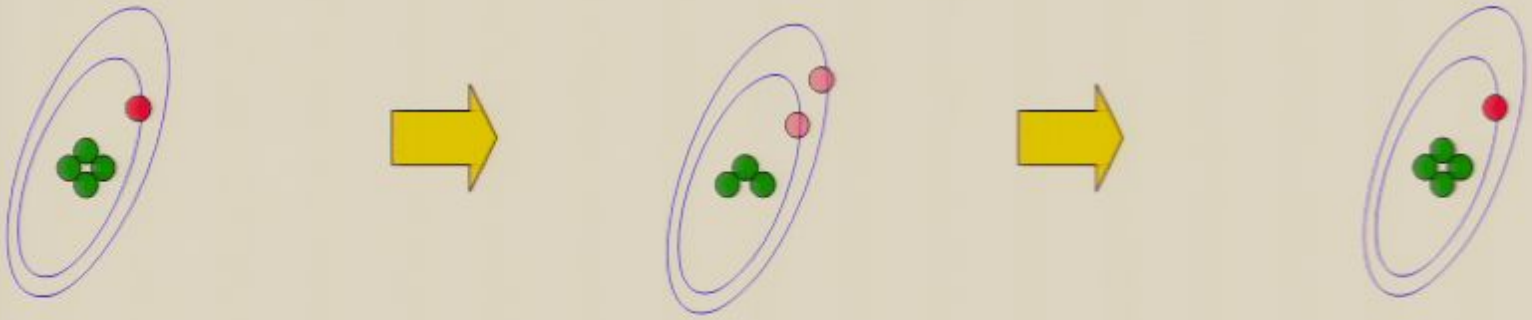
Another physical example



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


10^9
$15+10$

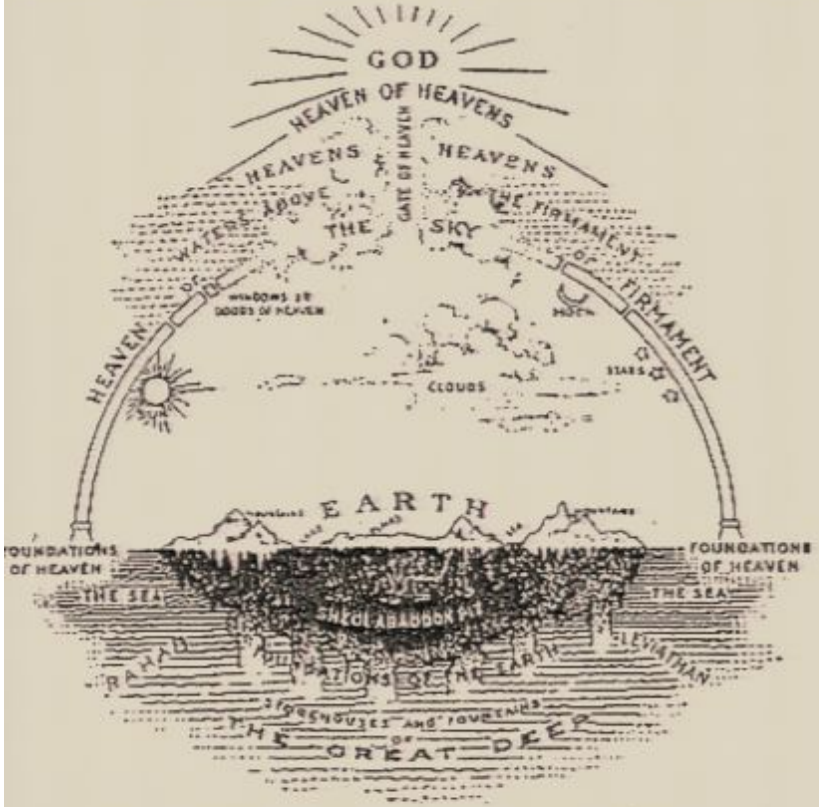
Another physical example



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

A new mathematical framework

The discovery of quantum mechanics was a revolution in our fundamental understanding of Nature.

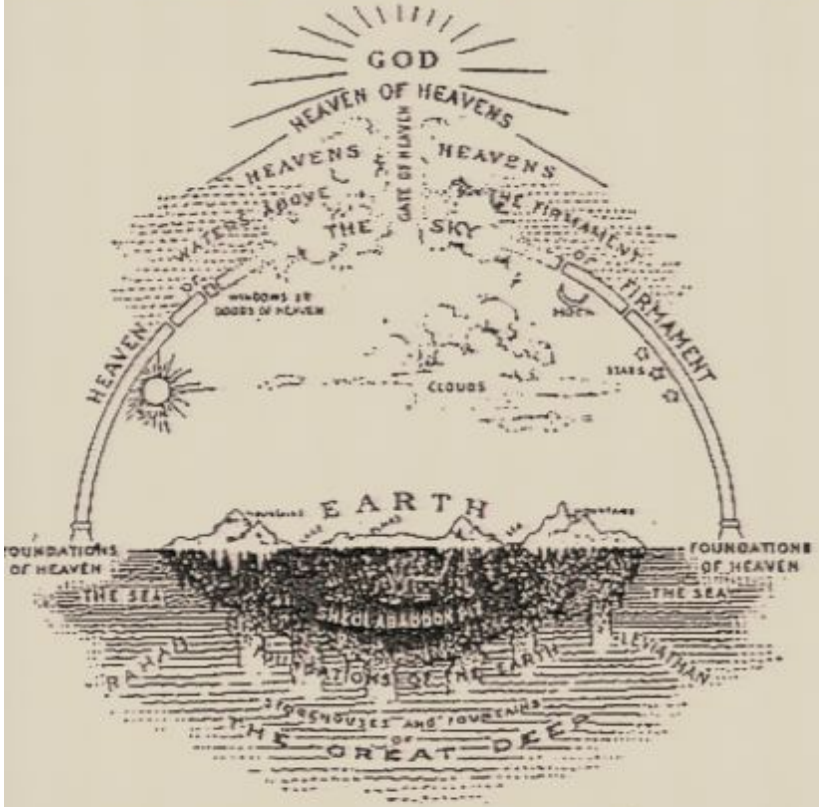


THE ANCIENT HEBREW CONCEPTION OF THE UNIVERSE

(analogy)

A new mathematical framework

The discovery of quantum mechanics was a revolution in our fundamental understanding of Nature.



THE ANCIENT HEBREW CONCEPTION OF THE UNIVERSE

(analogy)

Quantum mechanics and information

Quantum mechanics and information

Any physical medium capable of representing 0 and 1 is in principle capable of storing any linear combination $\alpha_0|0\rangle + \alpha_1|1\rangle$

Quantum mechanics and information

Any physical medium capable of representing 0 and 1 is in principle capable of storing any linear combination $\alpha_0|0\rangle + \alpha_1|1\rangle$

What does $\alpha_0|0\rangle + \alpha_1|1\rangle$ really mean??

Quantum mechanics and information

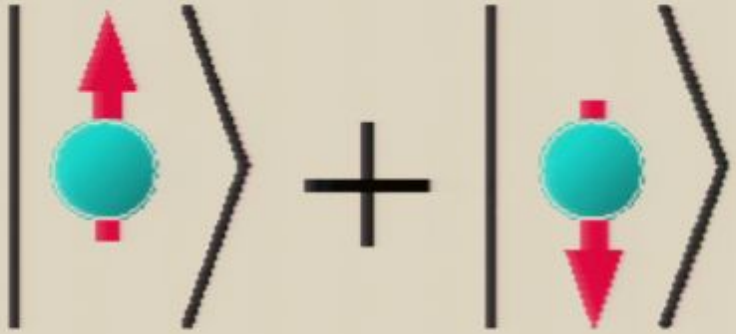
Any physical medium capable of representing 0 and 1 is in principle capable of storing any linear combination $\alpha_0|0\rangle + \alpha_1|1\rangle$

What does $\alpha_0|0\rangle + \alpha_1|1\rangle$ really mean??

t's a "mystery". THE mystery. We don't
nderstand it, but we can tell you how it works.
Feynman)

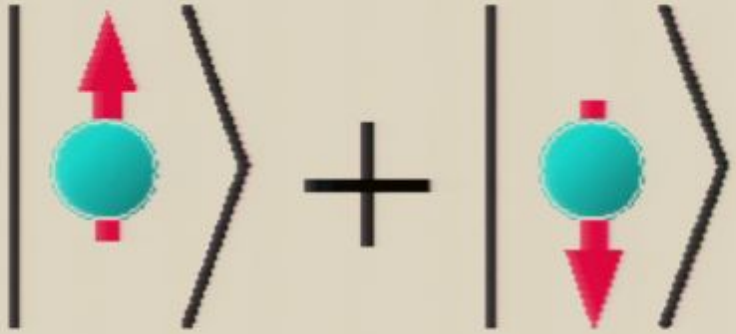
In a nutshell…

A system that can exist in 2 or more distinguishable states can exist in all those states at the same time.



In a nutshell...

A system that can exist in 2 or more distinguishable states can exist in all those states at the same time.



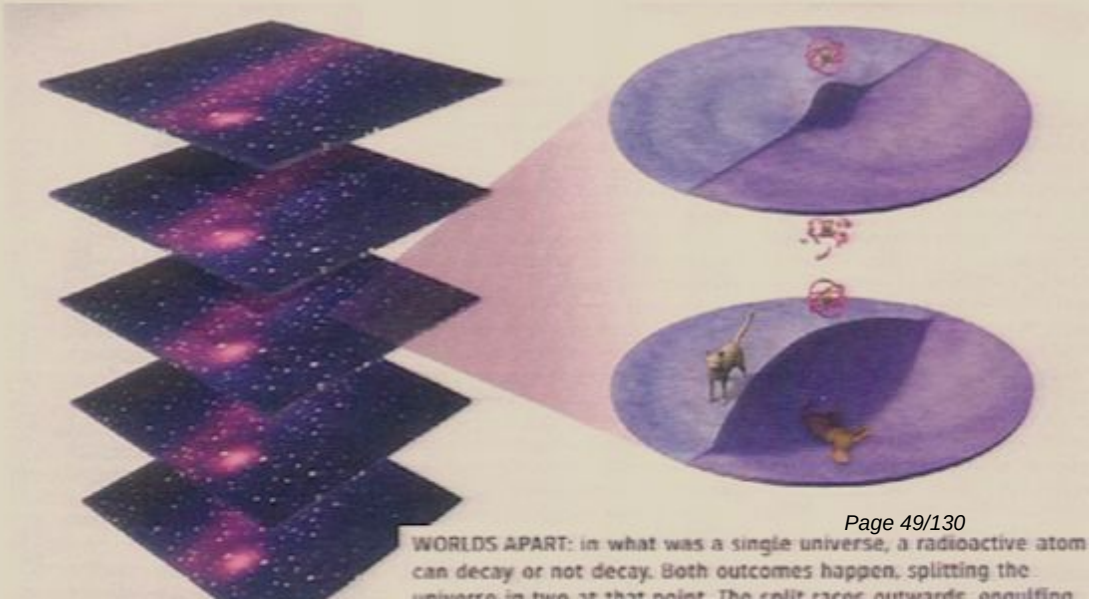
$$\frac{1}{\sqrt{2}}\left(\left|\text{cocktail}\right\rangle + \left|\text{beer}\right\rangle\right)$$

In a nutshell...

A system that can exist in 2 or more distinguishable states can exist in all those states at the same time.

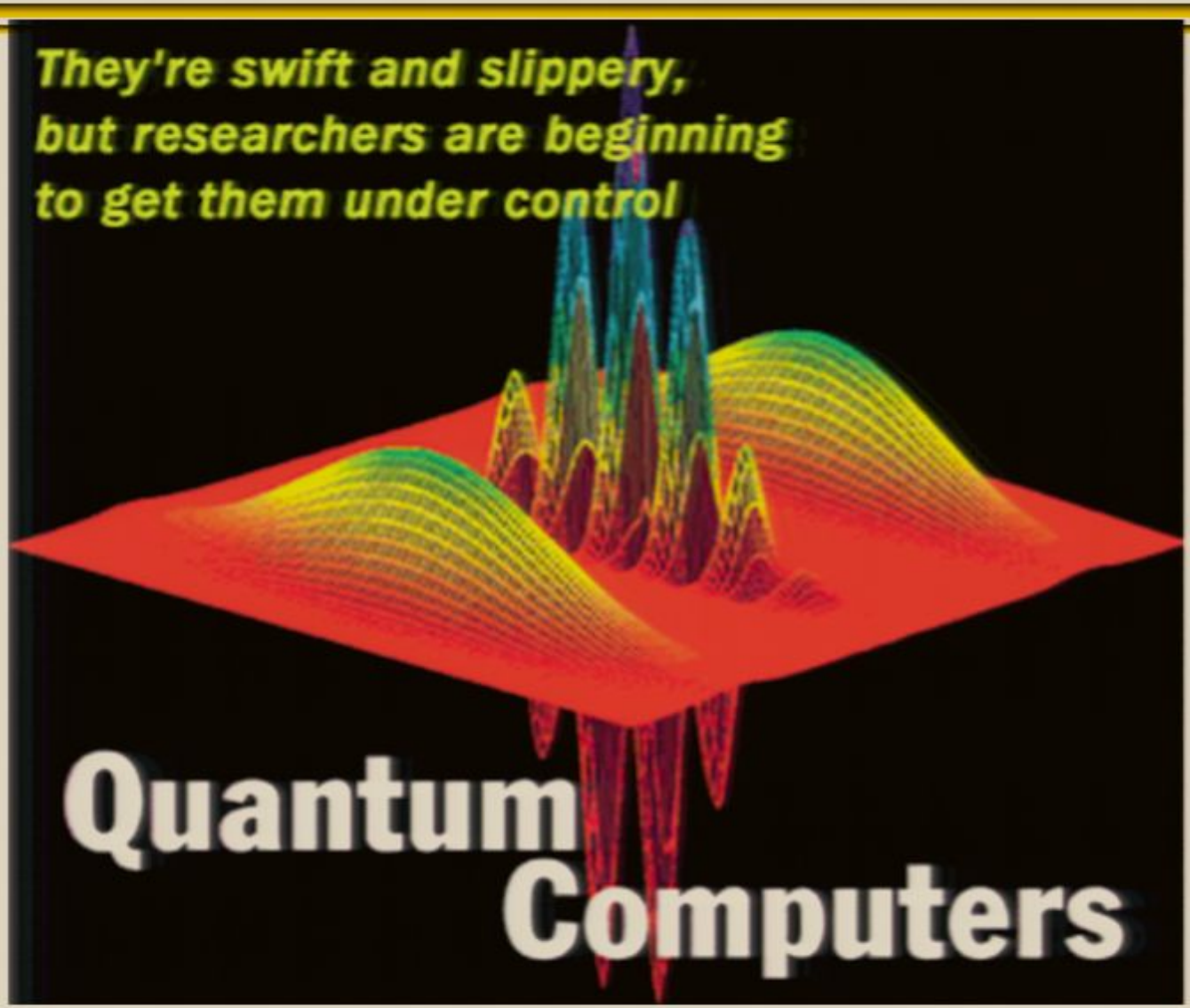
$$\left|\uparrow\right\rangle + \left|\downarrow\right\rangle$$

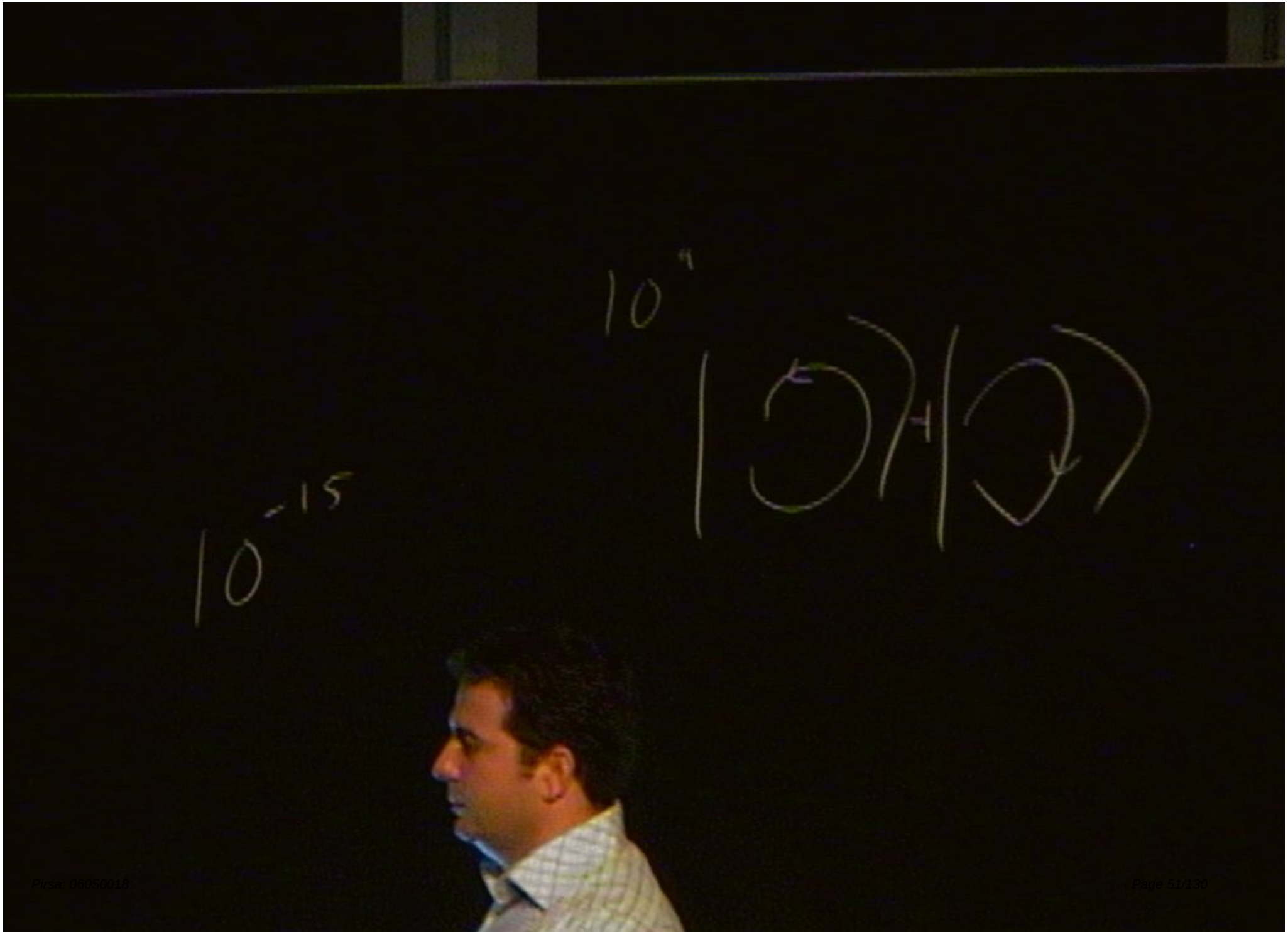
$$\frac{1}{\sqrt{2}}\left(\left|\text{cocktail}\right\rangle + \left|\text{beer}\right\rangle\right)$$



WORLDS APART: In what was a single universe, a radioactive atom can decay or not decay. Both outcomes happen, splitting the

Over the last century, scientists had moved from *observing* quantum phenomena to *controlling* them.

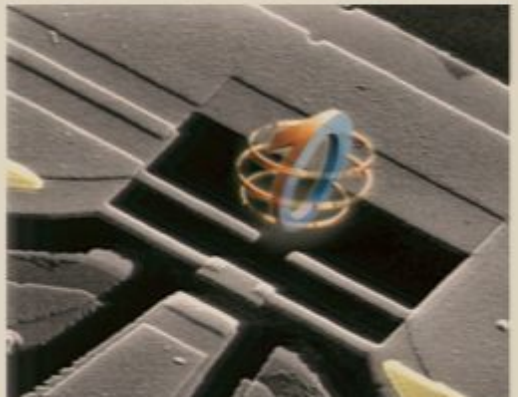



10^{9}
10^{-15}

Why is controlling quantum systems interesting?

Storing and manipulating information according to the laws of quantum theory, allows us to perform tasks previously thought to be impossible or infeasible.

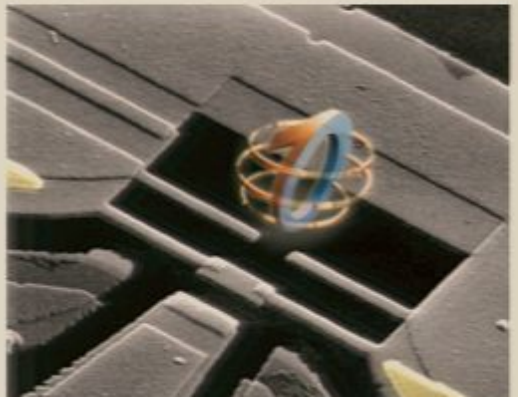
(contradicting the classical Church-Turing thesis)



Why is controlling quantum systems interesting?

Storing and manipulating information according to the laws of quantum theory, allows us to perform tasks previously thought to be impossible or infeasible.

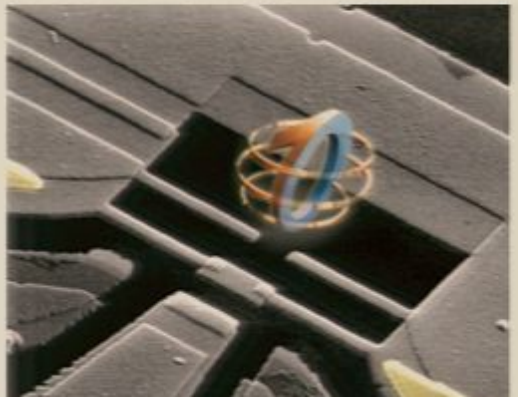
(contradicting the classical Church-Turing thesis)



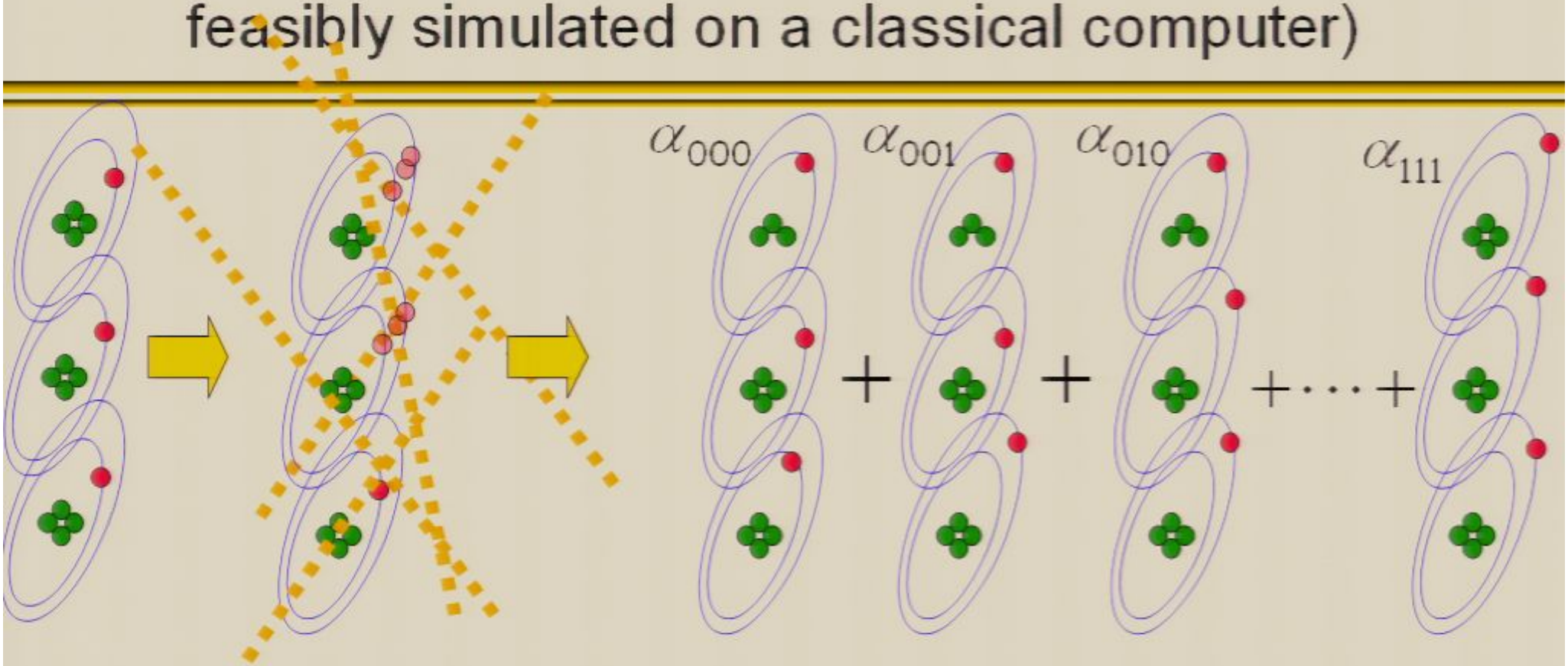
Why is controlling quantum systems interesting?

Storing and manipulating information according to the laws of quantum theory, allows us to perform tasks previously thought to be impossible or infeasible.

(contradicting the classical Church-Turing thesis)

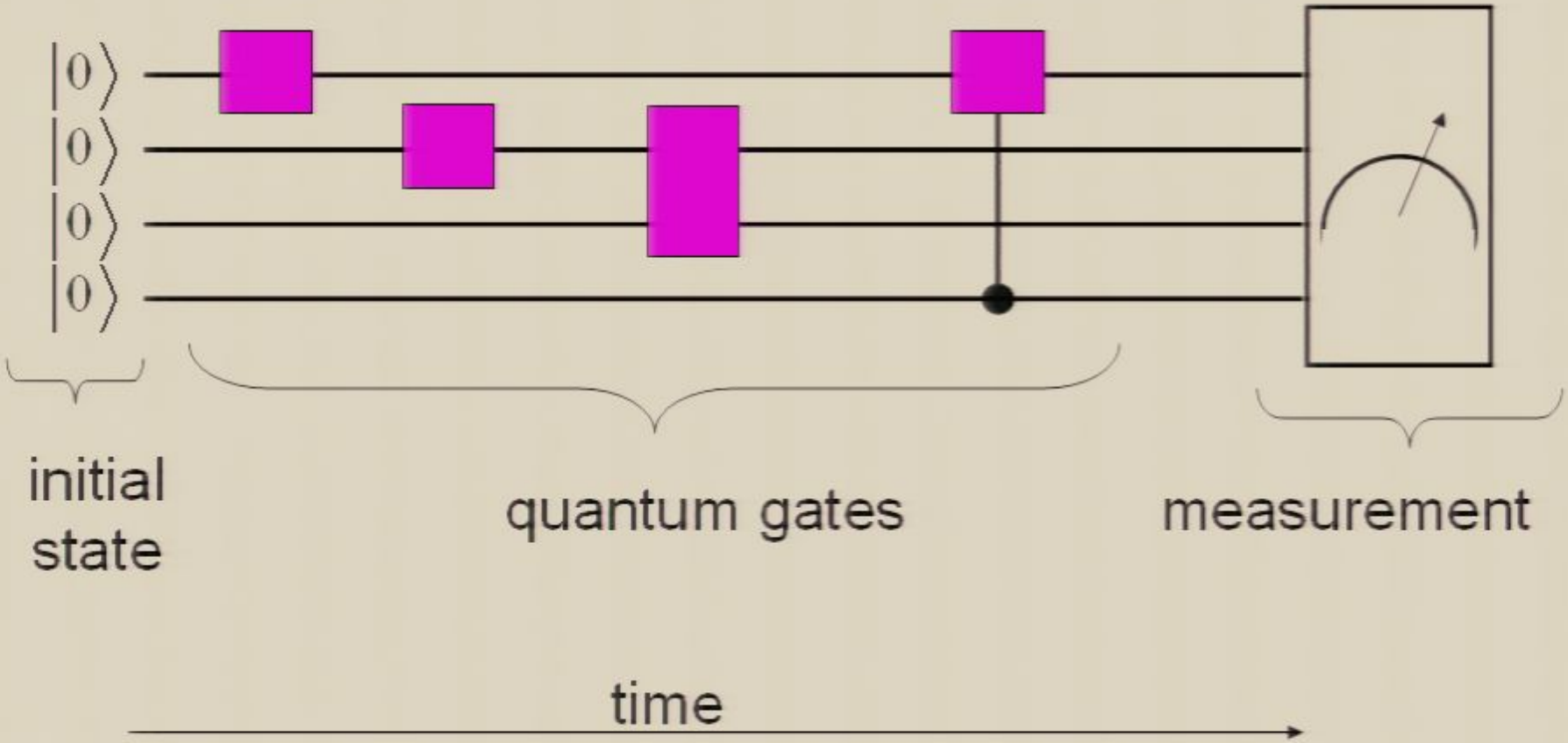


Quantum parallelism (cannot be feasibly simulated on a classical computer)

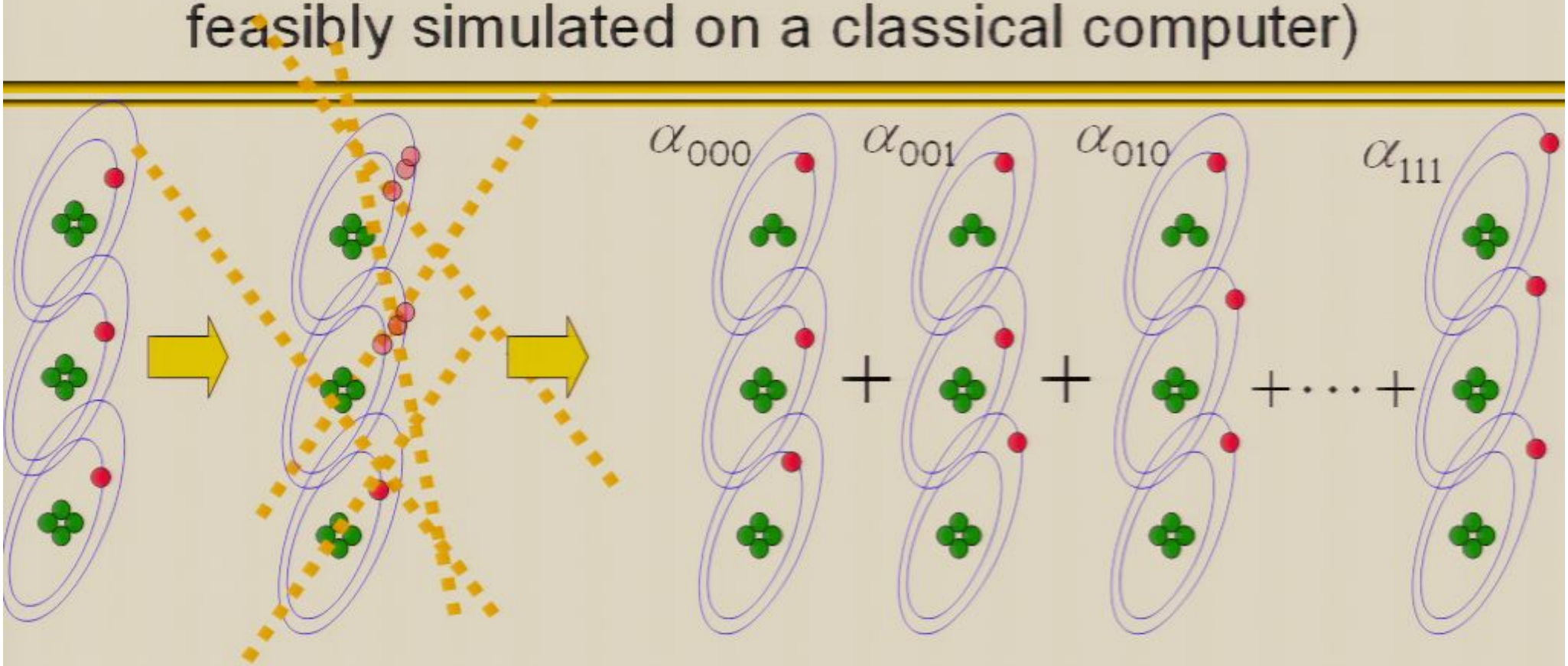


$$= \alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \cdots \alpha_{111}|111\rangle$$

A quantum circuit provides an visual representation of a quantum algorithm.

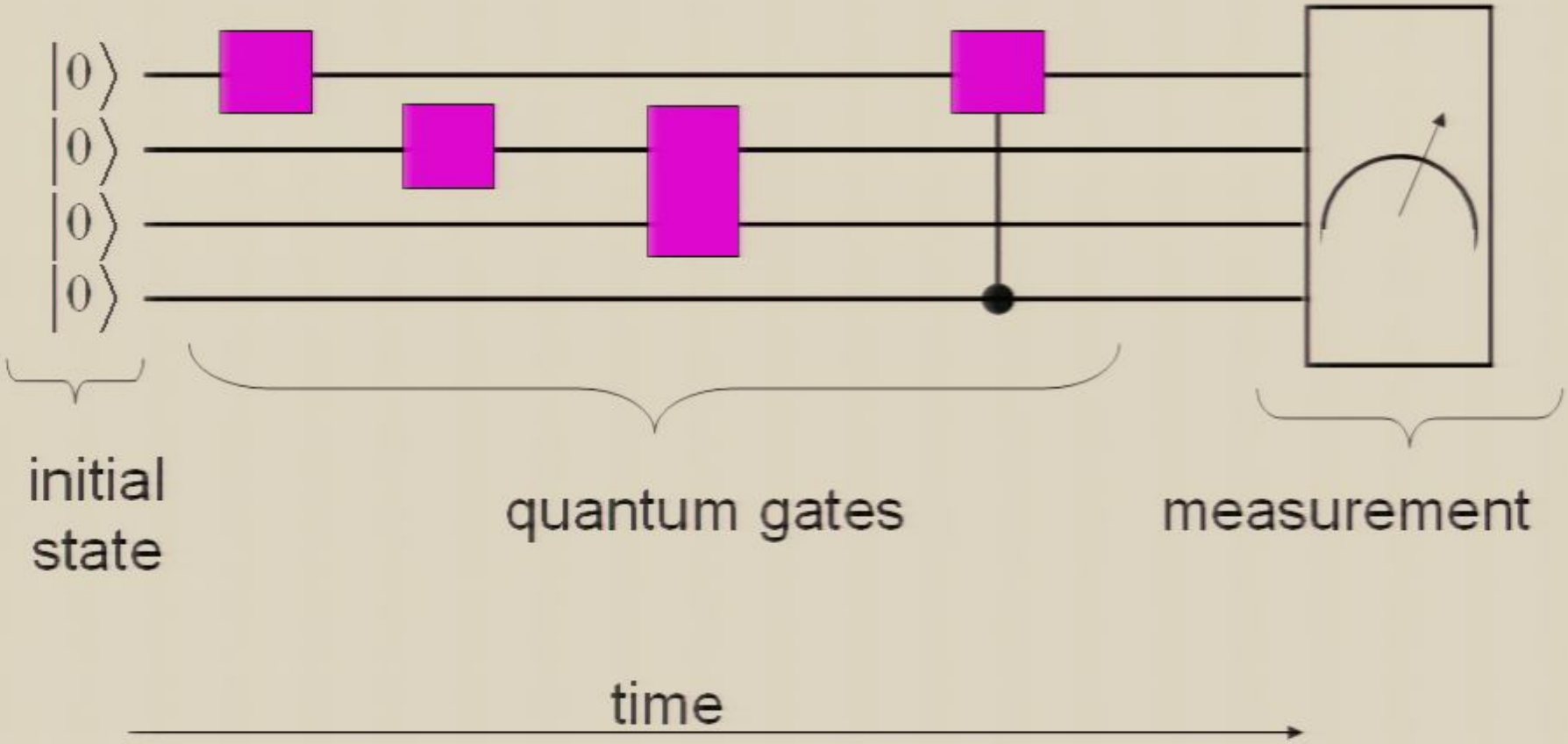


Quantum parallelism (cannot be feasibly simulated on a classical computer)



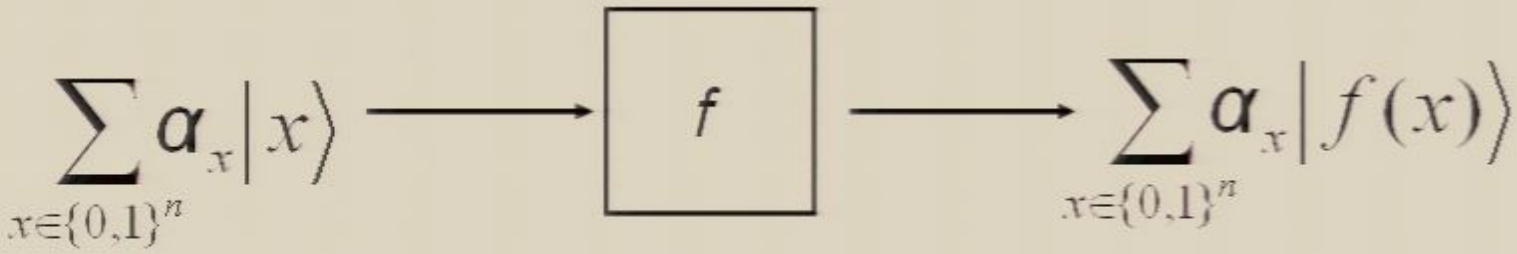
$$= \alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \cdots \alpha_{111}|111\rangle$$

A quantum circuit provides an visual representation of a quantum algorithm.



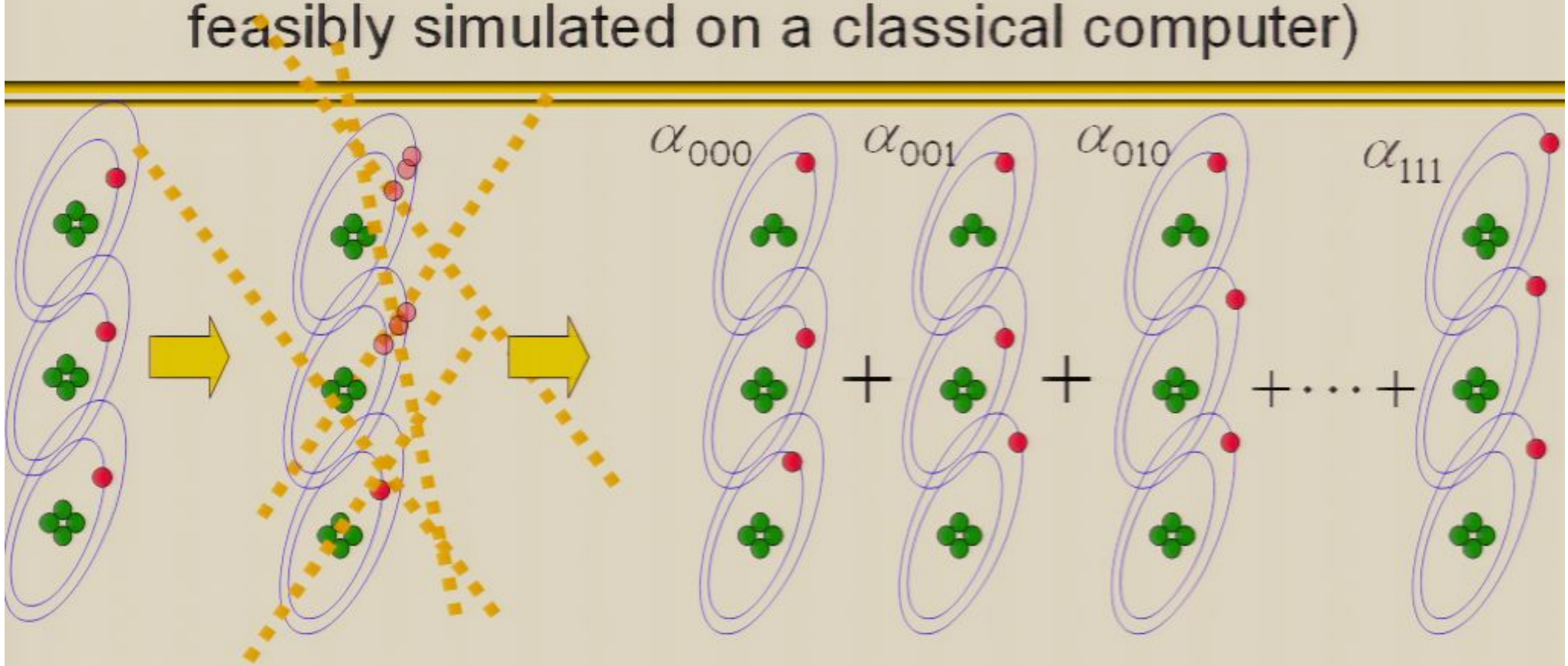
Quantum Parallelism

Since quantum states can exist in exponential superposition, a computation of a function being performed on *quantum states* can process an *exponential number of possible inputs* in a single evaluation of *f* :



By exploiting a phenomenon known as *quantum interference*, some *global properties* of *f* can be deduced from the output

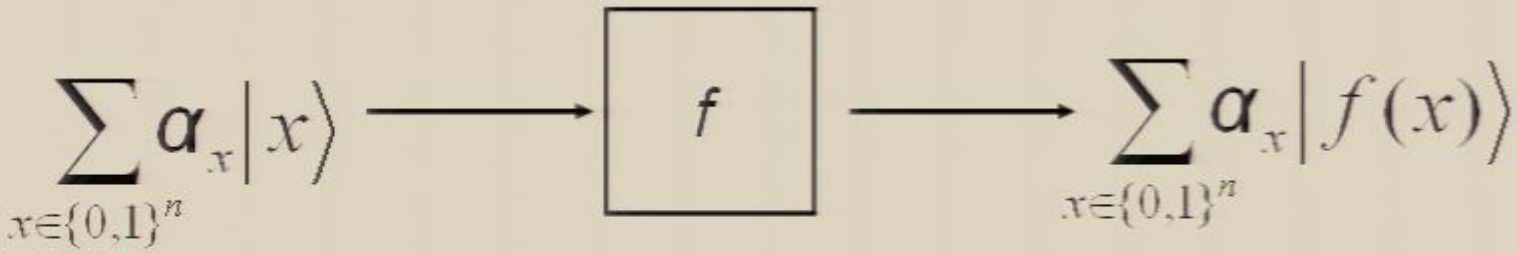
Quantum parallelism (cannot be feasibly simulated on a classical computer)



$$= \alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \cdots \alpha_{111}|111\rangle$$

Quantum Parallelism

Since quantum states can exist in exponential superposition, a computation of a function being performed on *quantum states* can process an *exponential number of possible inputs* in a single evaluation of *f* :



By exploiting a phenomenon known as *quantum interference*, some *global properties* of *f* can be deduced from the output

Applications

- Simulating quantum mechanical systems
- Factoring and Discrete Logs
- Hidden subgroup problems
- Amplitude amplification
- and more…

Quantum Algorithms

Integer Factorization (basis of RSA cryptography):

Given $N=pq$, find p and q.

Discrete logarithms (basis of DH crypto, including ECC):

$a,b \in G$, $a^k = b$, find k

Computational Complexity Comparison

	Classical	Quantum
Factoring	$e^{O\left(n^{1/3}\log^{2/3} n\right)}$	$O(n) \in e^{O(\log n)}$
Elliptic Curve Discrete Logarithms	$e^{O(n)}$	$O(n) \in e^{O(\log n)}$

(in terms of number of group multiplications, for n-bit inputs)

Amplitude Amplification

Consider any function $f : X \to \{0,1\}$.

Find x satisfying $f(x)=1$.

Suppose algorithm A succeeds with probability p.

With classical methods, we expect to repeat A a total of $1/p$ time before finding a solution, since each application of A "boosts" the probability of finding a solution by roughly p

$$\underbrace{p+p+p+p+p+p+p+p+p+p+\cdots}_{1/p} \approx 1$$

Amplitude Amplification

A quantum mechanical implementation of A succeeds with probability amplitude $\sqrt{p}$.

With quantum methods, each application of A "boosts" the probability amplitude of finding a solution by roughly $\sqrt{p}$

$$\underbrace{\sqrt{p}+\sqrt{p}+\sqrt{p}+\cdots}_{\sqrt{1/p}} \approx 1$$

i.e. we get a square root speedup!

A fundamental property of quantum mechanics: entanglement

Mathematically…

If we combine two qubits $\left(\alpha_1|0\rangle + \beta_1|1\rangle\right)$

and $\left(\alpha_2|0\rangle + \beta_2|1\rangle\right)$

We describe the joint system as

$$\left(\alpha_1|0\rangle + \beta_1|1\rangle\right)\left(\alpha_2|0\rangle + \beta_2|1\rangle\right)$$

$$= \alpha_1\alpha_2|0\rangle|0\rangle + \alpha_1\beta_2|0\rangle|1\rangle + \beta_1\alpha_2|1\rangle|0\rangle + \beta_1\beta_2|1\rangle|1\rangle$$

If the two qubits interact, their joint state can evolve into a superposition that cannot be factorized into two independent one-qubit states

e.g. “EPR pair” or “Bell pair”

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

If the two qubits interact, their joint state can evolve into a superposition that cannot be factorized into two independent one-qubit states

e.g. “EPR pair” or “Bell pair”

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

$$\neq \alpha_1\alpha_2|0\rangle|0\rangle + \alpha_1\beta_2|0\rangle|1\rangle + \beta_1\alpha_2|1\rangle|0\rangle + \beta_1\beta_2|1\rangle|1\rangle$$

Mathematically…

If we combine two qubits $\left(\alpha_1|0\rangle + \beta_1|1\rangle\right)$

and $\left(\alpha_2|0\rangle + \beta_2|1\rangle\right)$

We describe the joint system as

$$\left(\alpha_1|0\rangle + \beta_1|1\rangle\right)\left(\alpha_2|0\rangle + \beta_2|1\rangle\right)$$

$$= \alpha_1\alpha_2|0\rangle|0\rangle + \alpha_1\beta_2|0\rangle|1\rangle + \beta_1\alpha_2|1\rangle|0\rangle + \beta_1\beta_2|1\rangle|1\rangle$$

If the two qubits interact, their joint state can evolve into a superposition that cannot be factorized into two independent one-qubit states

e.g. “EPR pair” or “Bell pair”

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

$$\neq \alpha_1\alpha_2|0\rangle|0\rangle + \alpha_1\beta_2|0\rangle|1\rangle + \beta_1\alpha_2|1\rangle|0\rangle + \beta_1\beta_2|1\rangle|1\rangle$$

A simple application of entanglement: quantum teleportation

Mathematically…

A simple computation will verify that

$$(\alpha|0\rangle+\beta|1\rangle)\left(\frac{1}{\sqrt{2}}|0\rangle|0\rangle+\frac{1}{\sqrt{2}}|1\rangle|1\rangle\right)$$

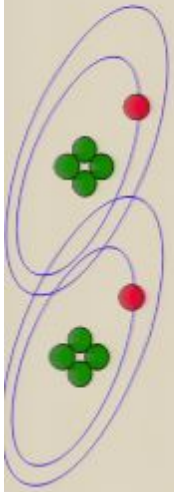
$$=\frac{1}{2}(|0\rangle|0\rangle+|1\rangle|1\rangle)(\alpha|0\rangle+\beta|1\rangle)$$

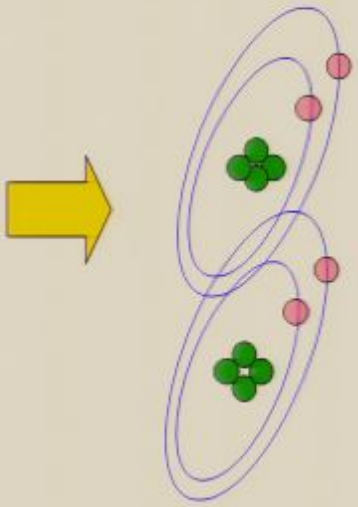
$$+\frac{1}{2}(|0\rangle|0\rangle-|1\rangle|1\rangle)(\alpha|0\rangle-\beta|1\rangle)$$

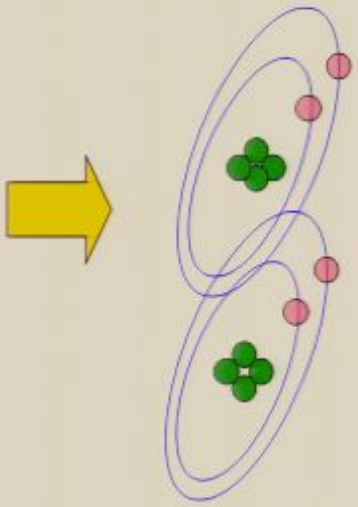
$$+\frac{1}{2}(|0\rangle|1\rangle+|1\rangle|0\rangle)(\alpha|1\rangle+\beta|0\rangle)$$

So what??

$$+\frac{1}{2}(|0\rangle|1\rangle-|1\rangle|0\rangle)(\alpha|1\rangle-\beta|0\rangle)$$







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

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

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

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

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

$$= (\alpha|0\rangle + \beta|1\rangle)\left(\frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle\right)$$

$$= \frac{1}{2}\left(|0\rangle|0\rangle + |1\rangle|1\rangle\right)\left(\alpha|0\rangle + \beta|1\rangle\right)$$

$$+ \frac{1}{2}\left(|0\rangle|0\rangle - |1\rangle|1\rangle\right)\left(\alpha|0\rangle - \beta|1\rangle\right)$$

$$+ \frac{1}{2}\left(|0\rangle|1\rangle + |1\rangle|0\rangle\right)\left(\alpha|1\rangle + \beta|0\rangle\right)$$

$$+ \frac{1}{2}\left(|0\rangle|1\rangle - |1\rangle|0\rangle\right)\left(\alpha|1\rangle - \beta|0\rangle\right)$$


BUT BOB... IN A QUANTUM WORLD HOW CAN WE BE SURE
ψ⁺ or ψ⁻?

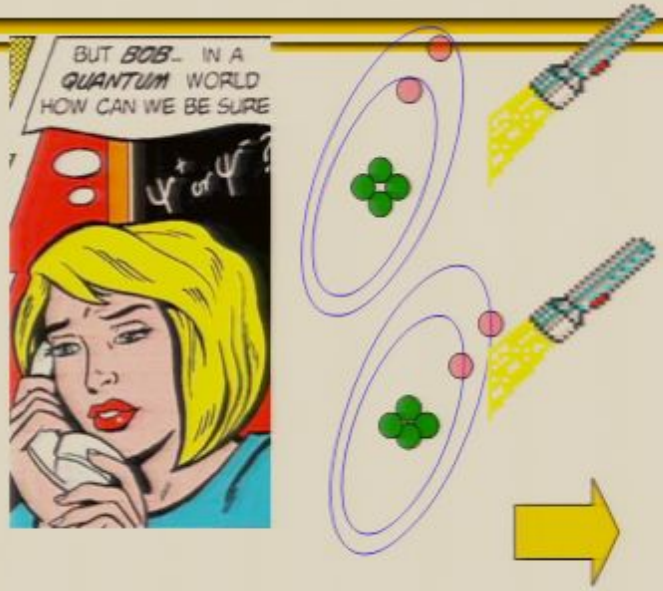

OH ALICE... YOU'RE THE ONE FOR ME

$$= \frac{1}{2}|0\rangle|0\rangle(\alpha|0\rangle + \beta|1\rangle)$$

$$+ \frac{1}{2}|0\rangle|1\rangle(\alpha|0\rangle - \beta|1\rangle)$$

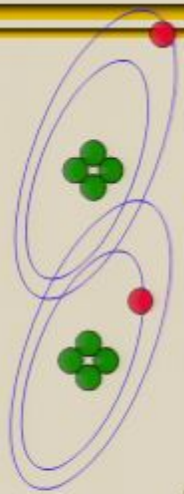
$$+ \frac{1}{2}|1\rangle|0\rangle(\alpha|1\rangle + \beta|0\rangle)$$

$$+ \frac{1}{2}|1\rangle|1\rangle(\alpha|1\rangle - \beta|0\rangle)$$

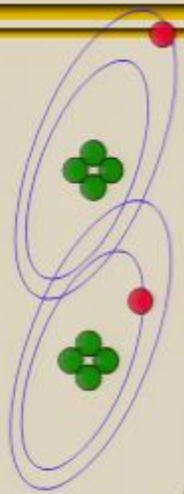

BUT BOB... IN A QUANTUM WORLD HOW CAN WE BE SURE
ψ⁺ or ψ⁻ ?


OH ALICE... YOU'RE THE ONE FOR ME


BUT BOB... IN A QUANTUM WORLD HOW CAN WE BE SURE
ψ+ or ψ-?




OH ALICE... YOU'RE THE ONE FOR ME



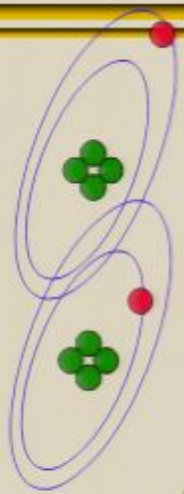
$$|1\rangle|0\rangle(\alpha|1\rangle+\beta|0\rangle)$$ with probability 25%

$$= \frac{1}{2}|0\rangle|0\rangle(\alpha|0\rangle + \beta|1\rangle)$$

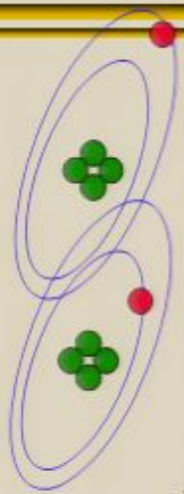
$$+ \frac{1}{2}|0\rangle|1\rangle(\alpha|0\rangle - \beta|1\rangle)$$

$$+ \frac{1}{2}|1\rangle|0\rangle(\alpha|1\rangle + \beta|0\rangle)$$

$$+ \frac{1}{2}|1\rangle|1\rangle(\alpha|1\rangle - \beta|0\rangle)$$

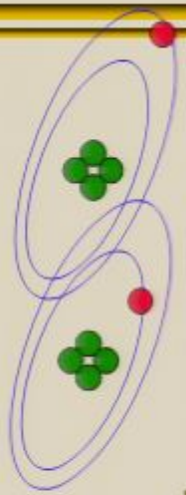


$$|1\rangle|0\rangle(\alpha|1\rangle+\beta|0\rangle)$$ with probability 25%

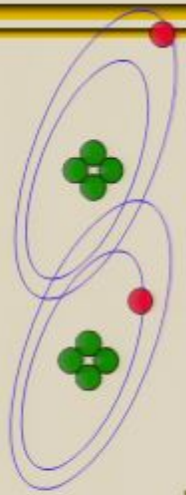


$$|1\rangle|0\rangle$$

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

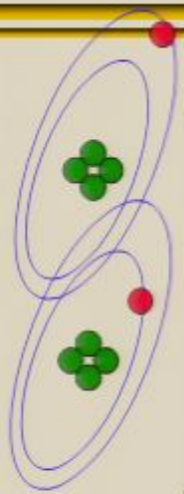


$$|1\rangle|0\rangle(\alpha|1\rangle+\beta|0\rangle)$$ with probability 25%



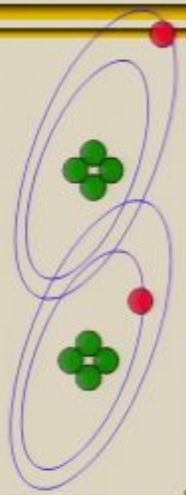
$$|1\rangle|0\rangle$$

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



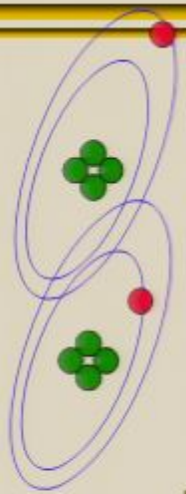
$|1\rangle|0\rangle$

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



$$|1\rangle|0\rangle$$

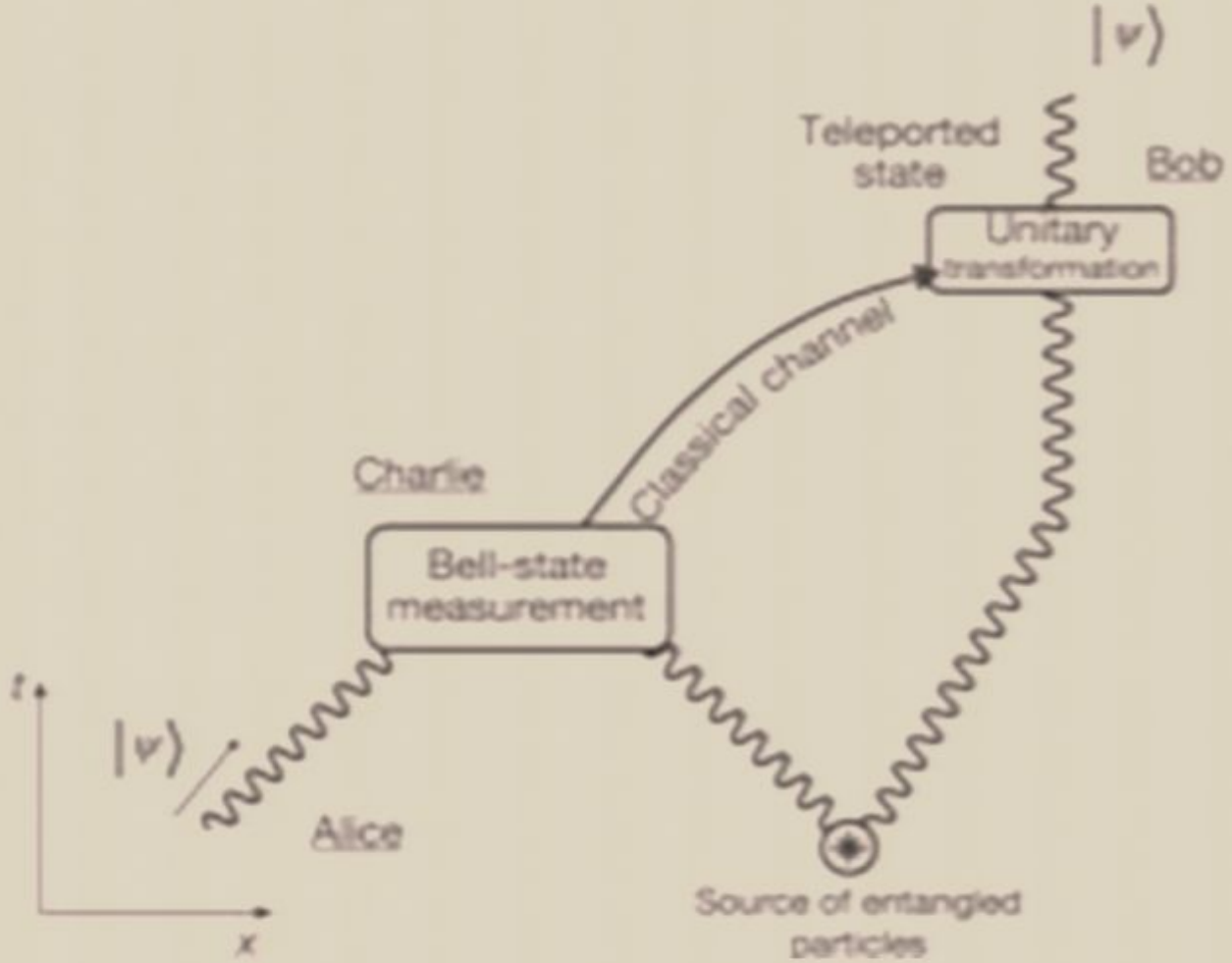
$$\alpha|1\rangle + \beta|0\rangle$$



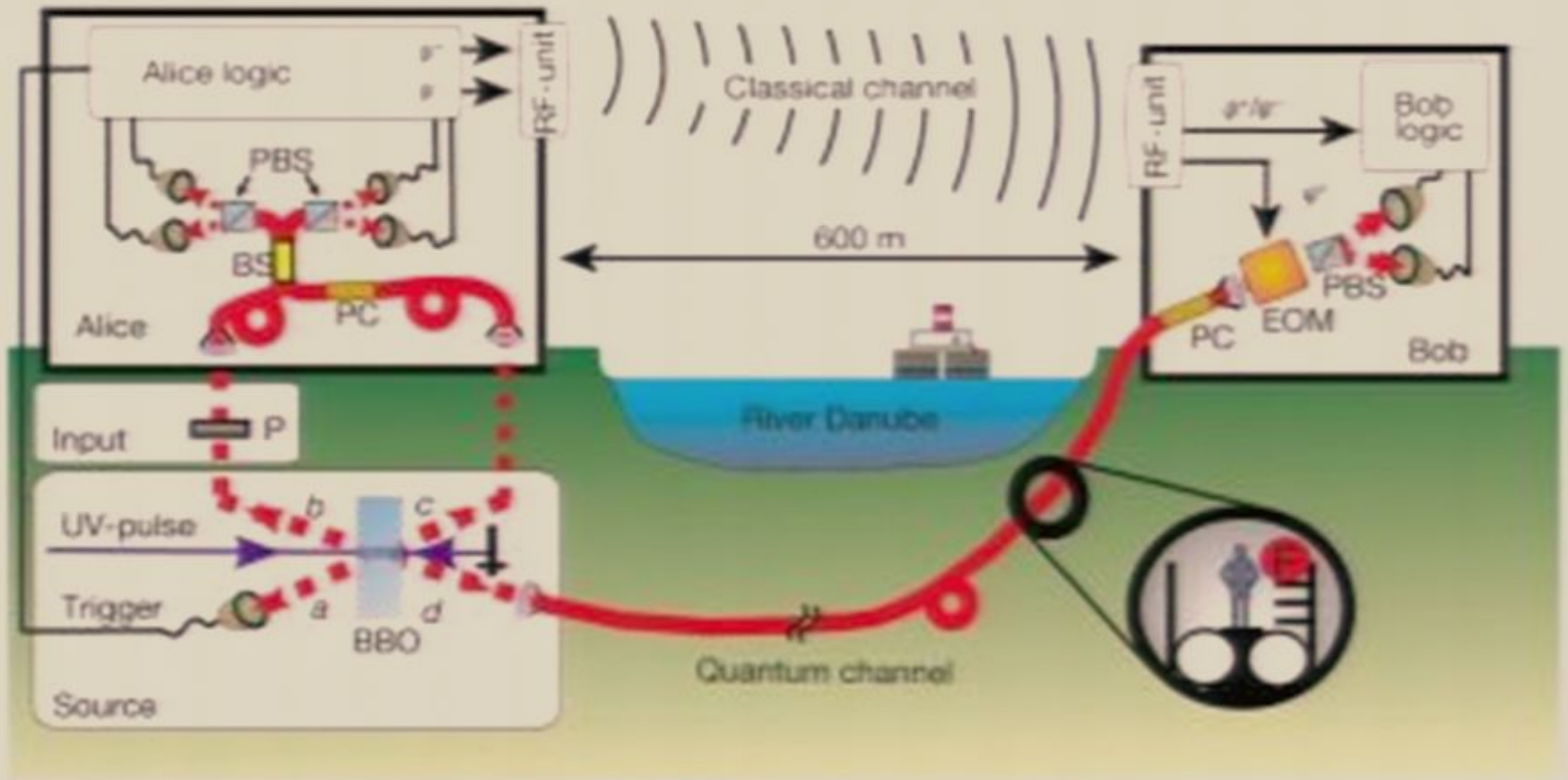
$$|1\rangle|0\rangle$$

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

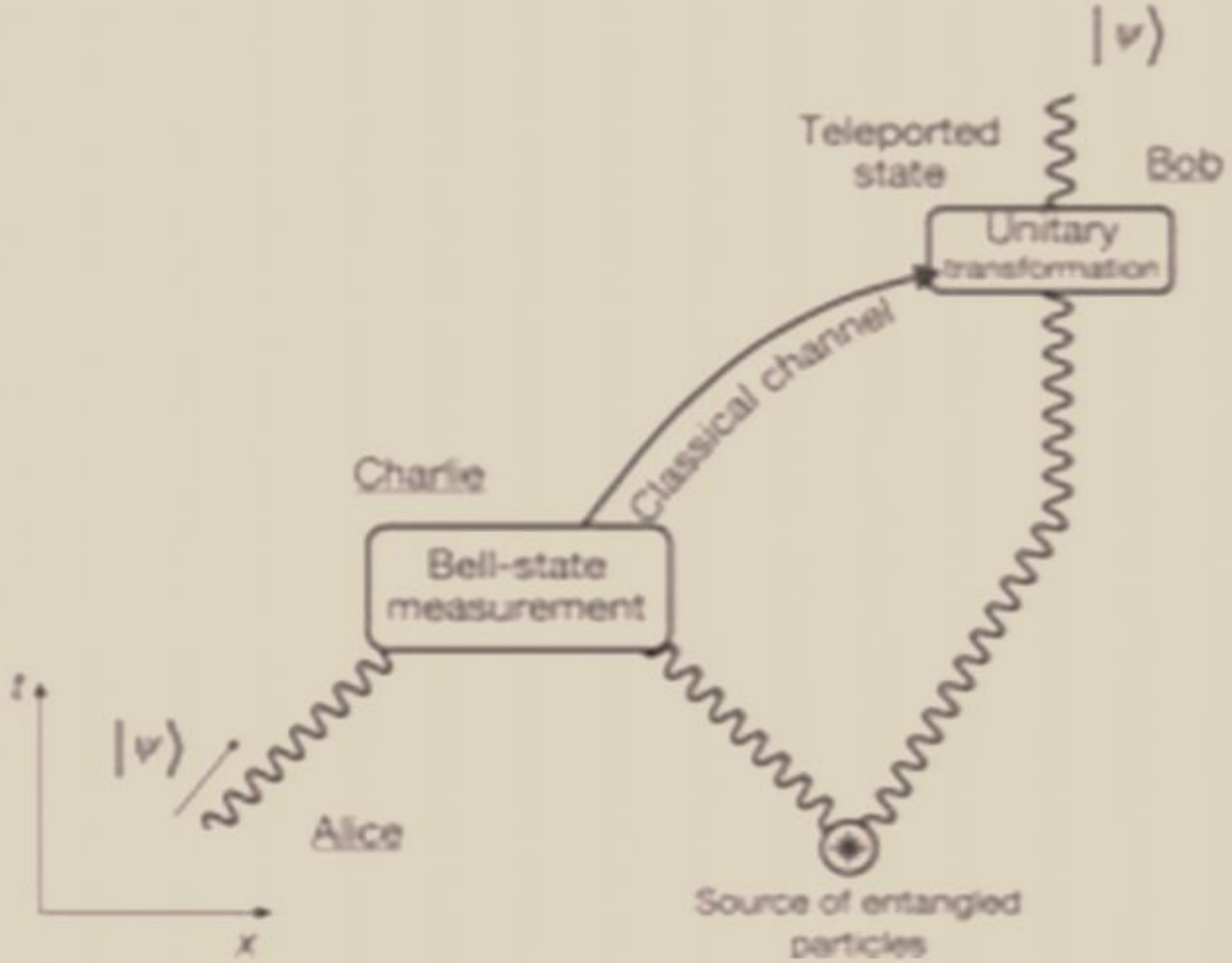
Original conception



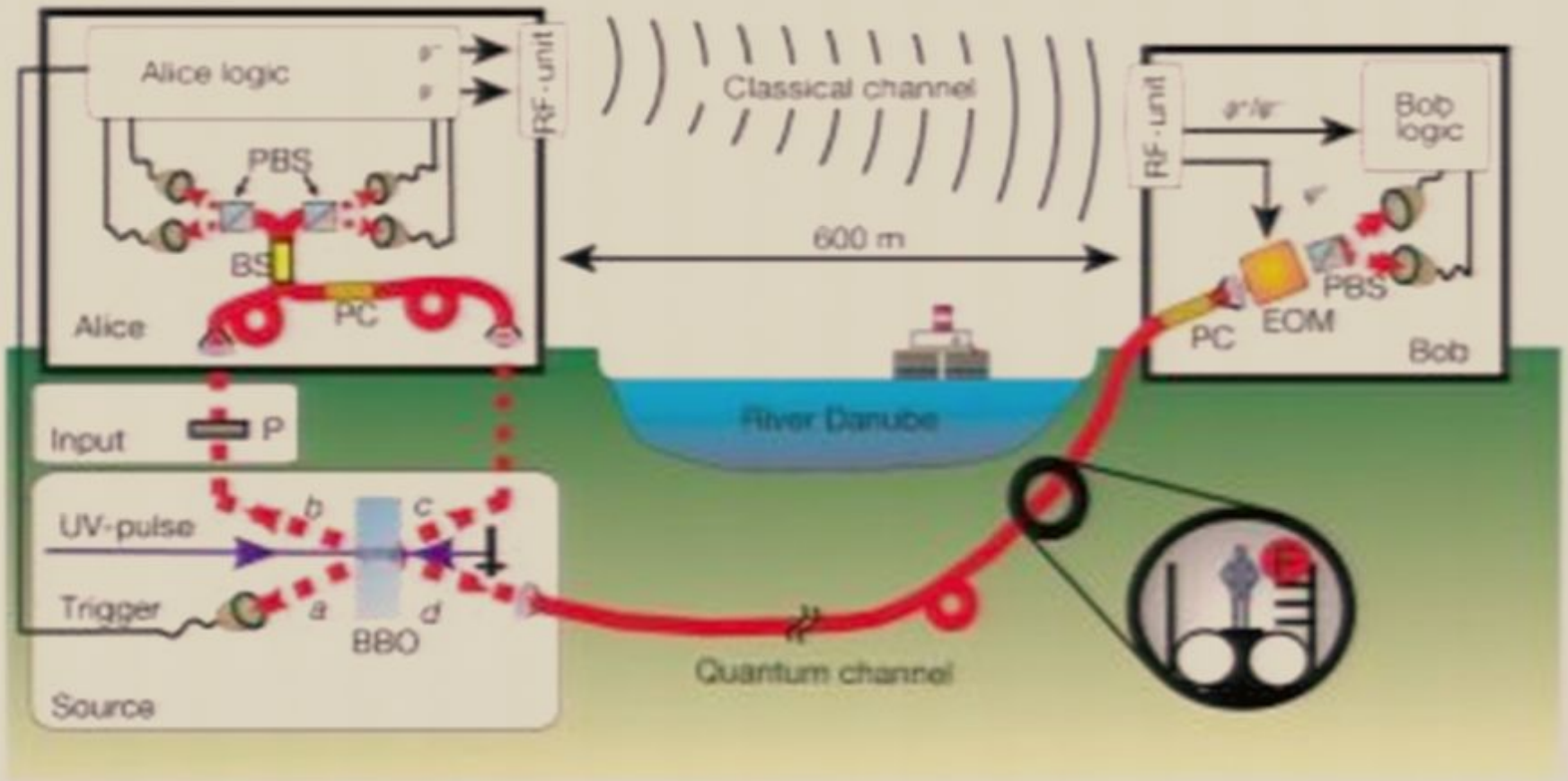
Actual implementations



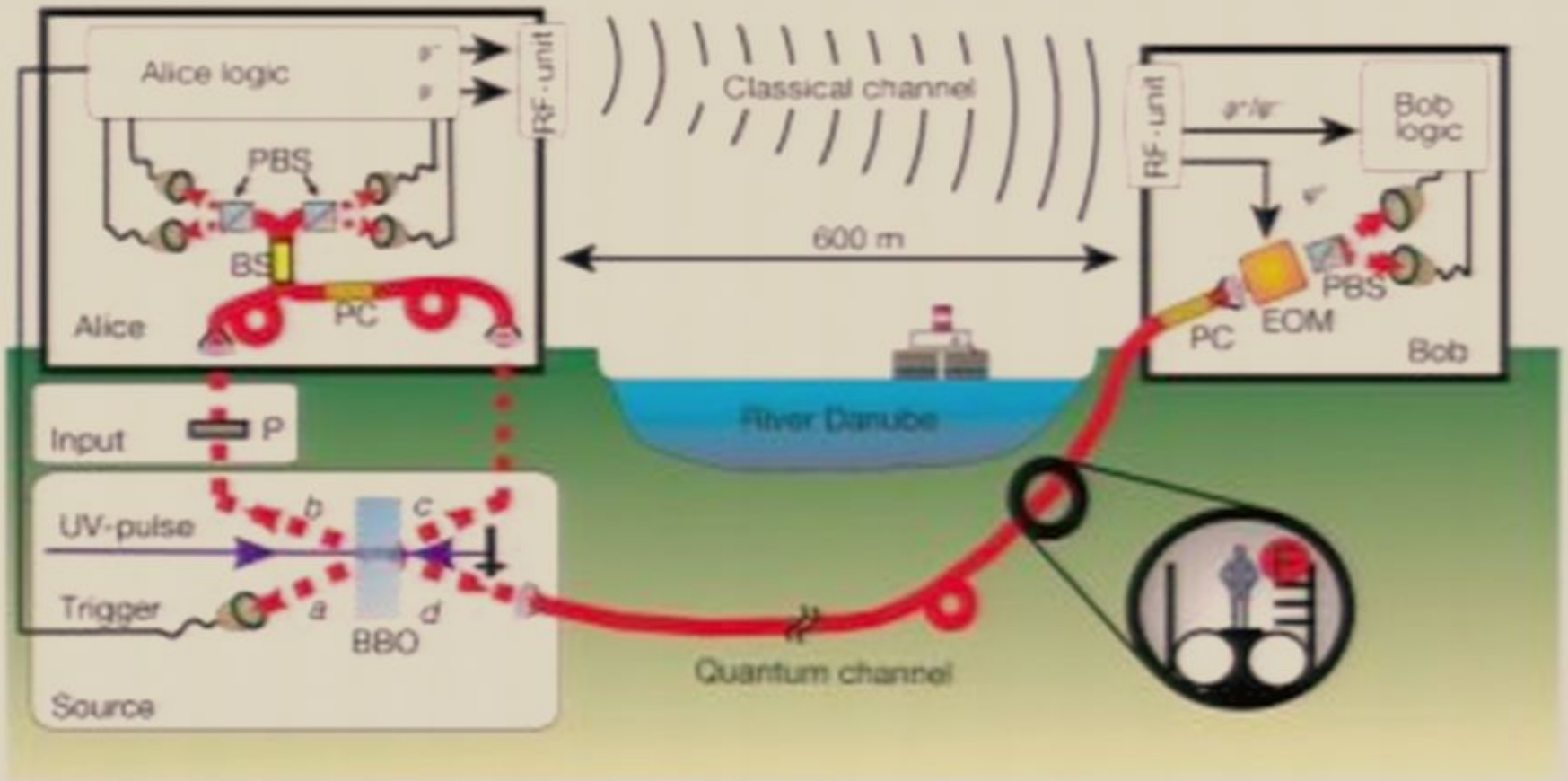
Original conception



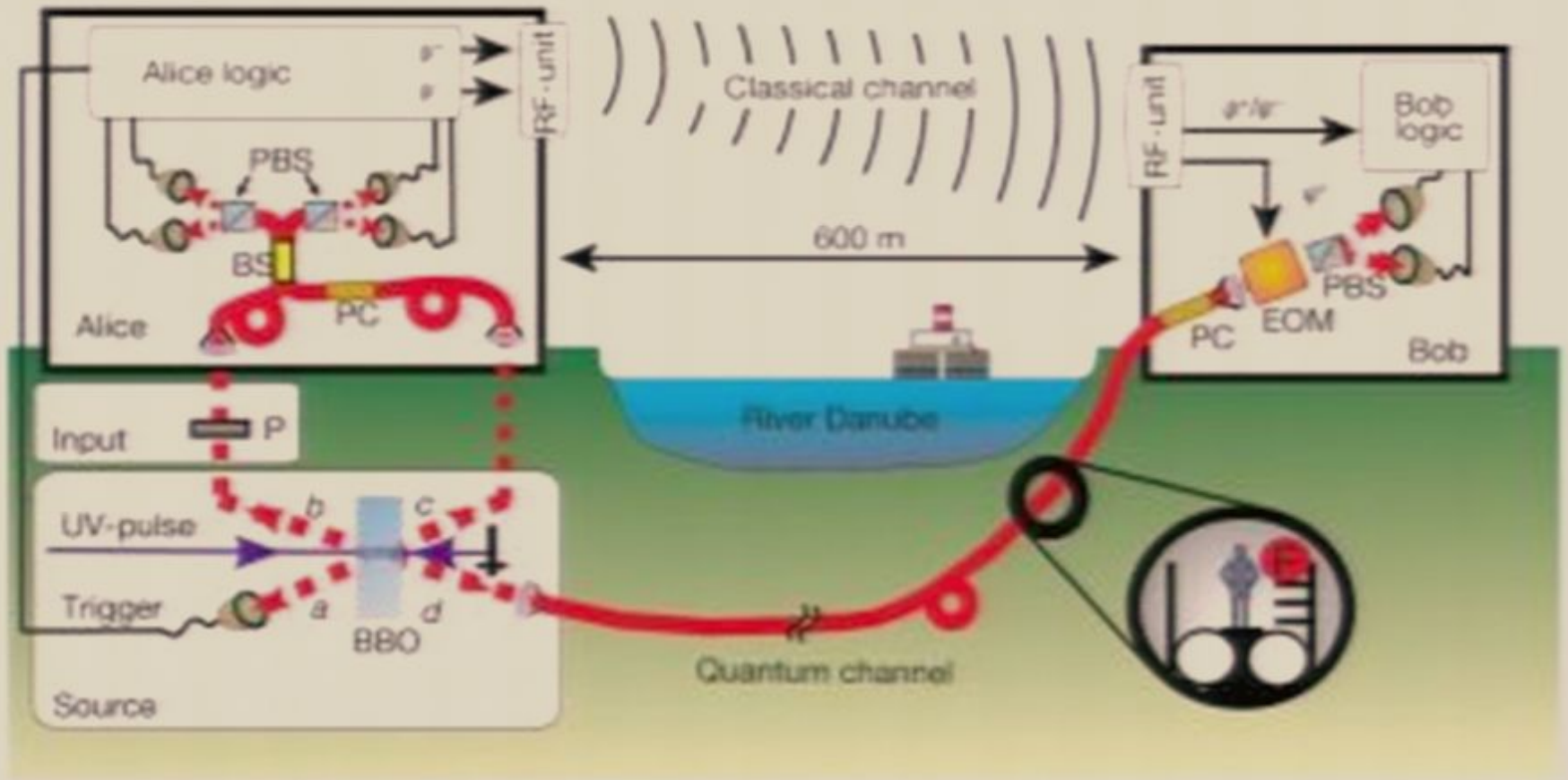
Actual implementations



Actual implementations



Actual implementations



Quantum Cryptography

Quantum Information Security

Quantum Information Security

- Quantum mechanics provides intrinsic eavesdropper detection.

Quantum Information Security

- Quantum mechanics provides intrinsic eavesdropper detection.
- e.g. no-cloning theorem: there is no transformation that will copy an unknown quantum state, i.e.

$$|\psi\rangle|0\rangle|workspace\rangle \mapsto |\psi\rangle|\psi\rangle|junk(\psi)\rangle$$

is not possible.

Quantum Information Security

Quantum Information Security

- More generally, any procedure that extracts information about an unknown quantum state, MUST disturb the state (on average)

Quantum Information Security

- More generally, any procedure that extracts information about an unknown quantum state, MUST disturb the state (on average)
- There is a fundamental quantifiable tradeoff between information extraction and disturbance.

Quantum Key Distribution (general idea)

quantum bits

Alice and Bob measure their qubits

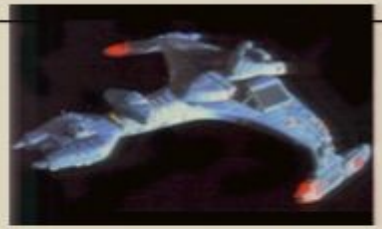
Authenticated public channel

Quantum Information Security

- More generally, any procedure that extracts information about an unknown quantum state, MUST disturb the state (on average)
- There is a fundamental quantifiable tradeoff between information extraction and disturbance.

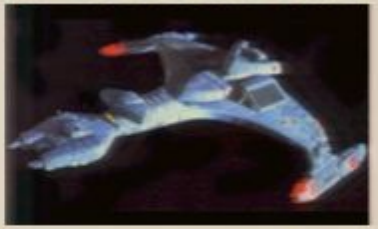
Quantum Key Distribution (general idea)

quantum bits



Alice and Bob measure their qubits

Authenticated public channel

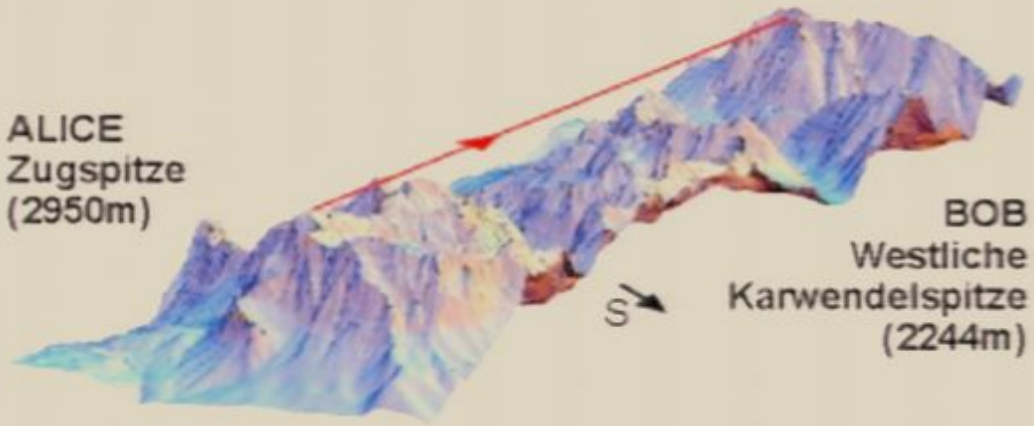


Quantum Key Distribution (general idea)

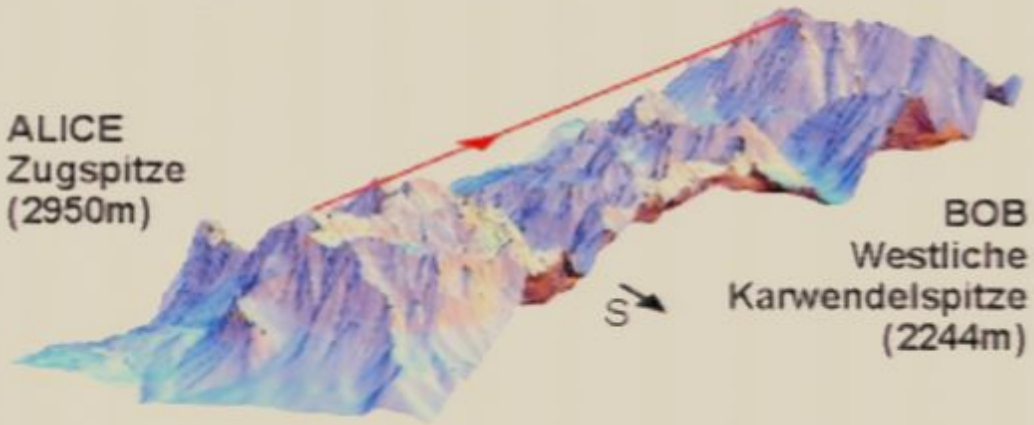
Alice and Bob publicly discuss the information they measured to assess how much information Eve could have obtained.

If Eve's information is very likely to be below a certain constant threshold, they can communicate further and distill out a very private shared key ("privacy amplification"). Otherwise they abandon the key.

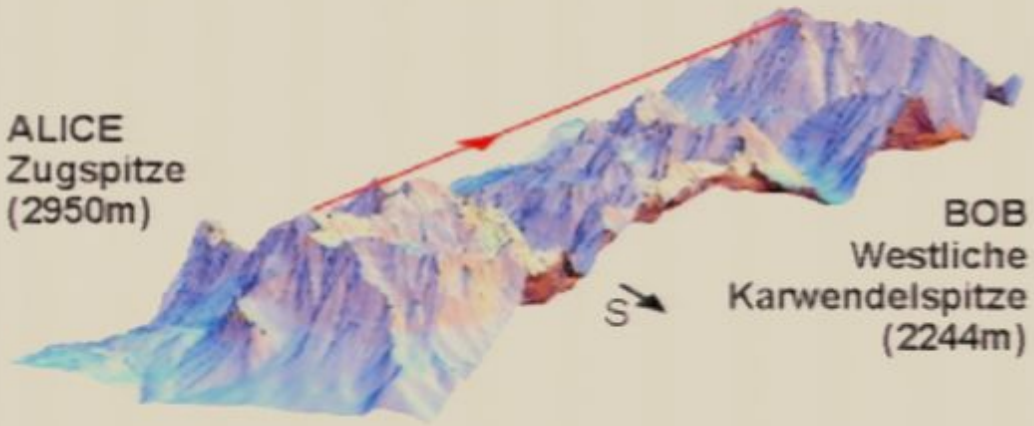
Quantum Key Distribution Implementations around the world



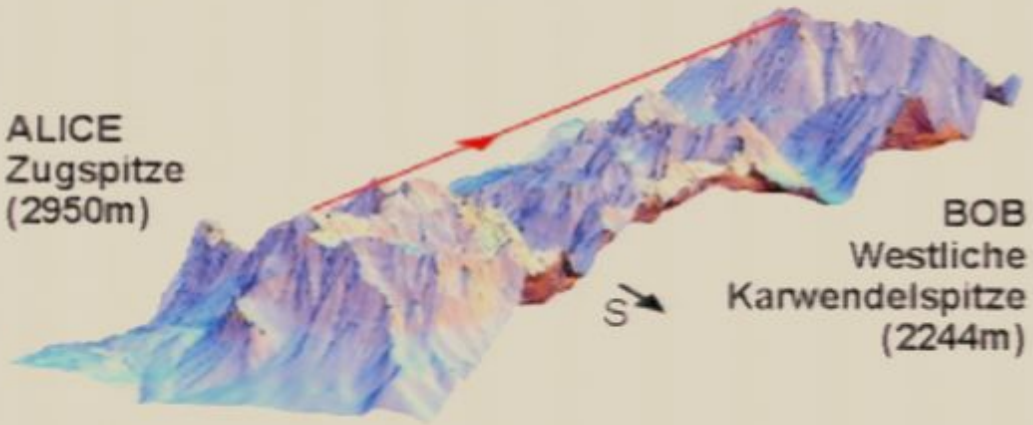
Quantum Key Distribution Implementations around the world



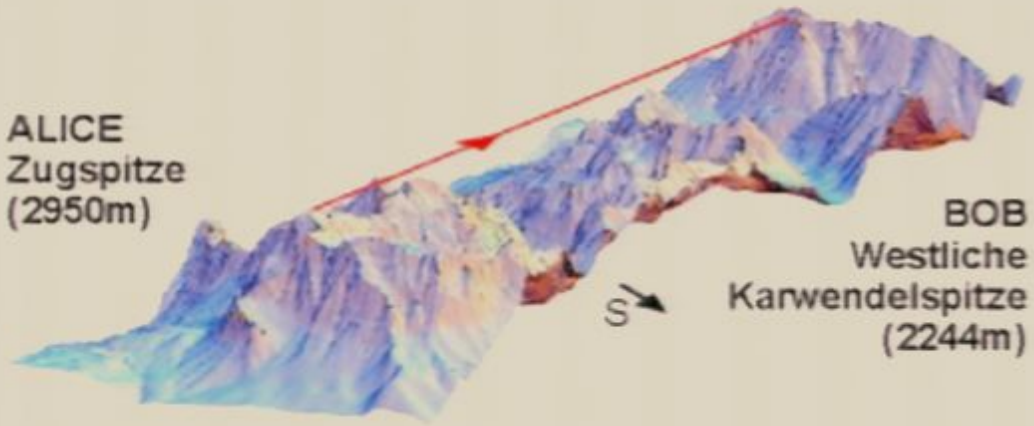
Quantum Key Distribution Implementations around the world



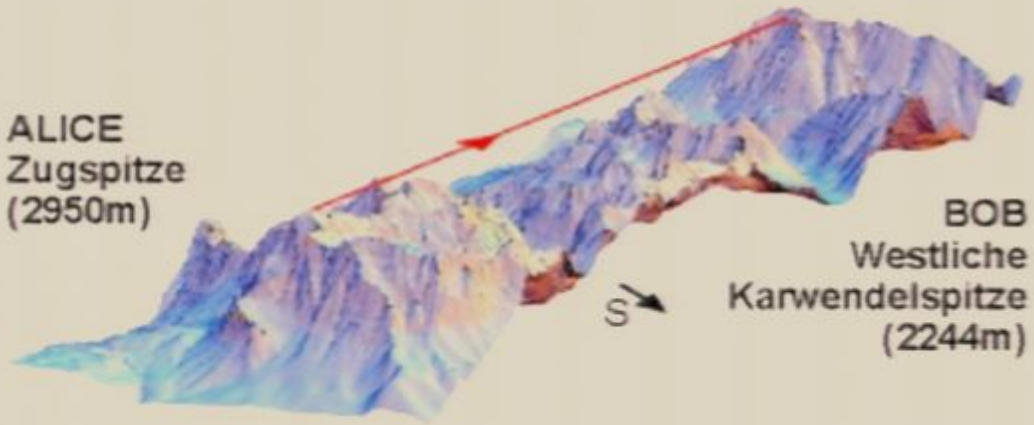
Quantum Key Distribution Implementations around the world



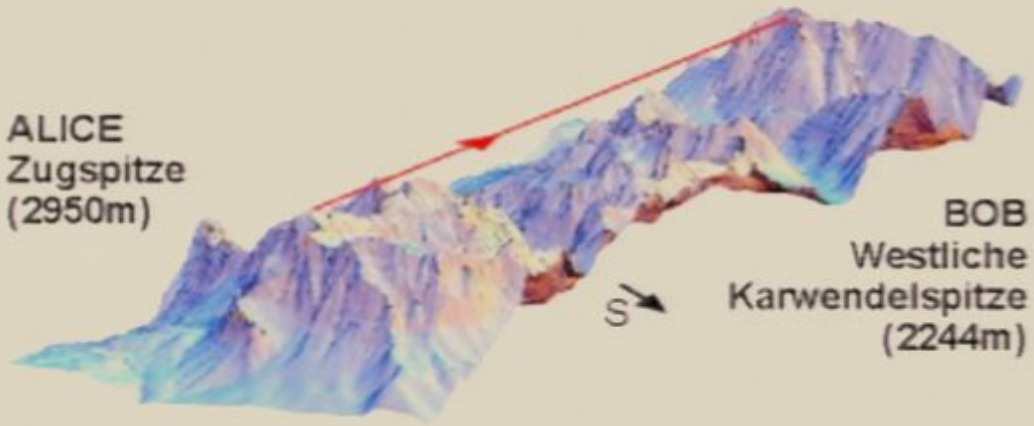
Quantum Key Distribution Implementations around the world



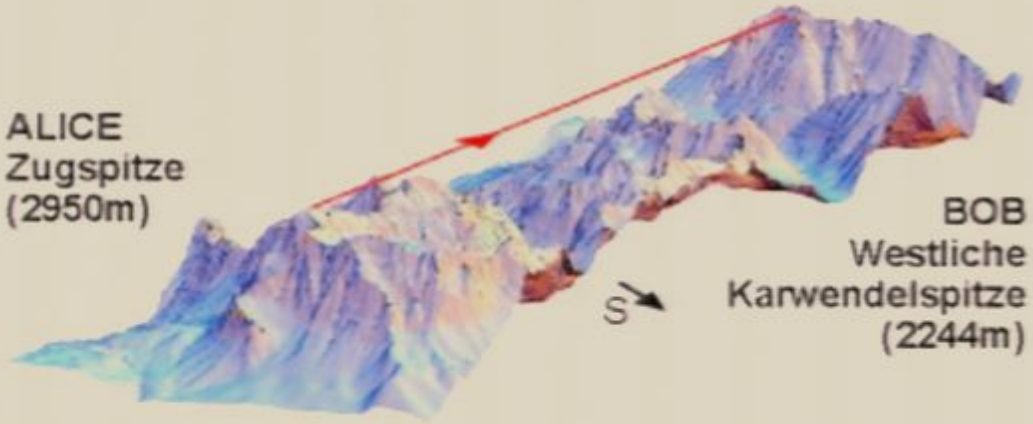
Quantum Key Distribution Implementations around the world



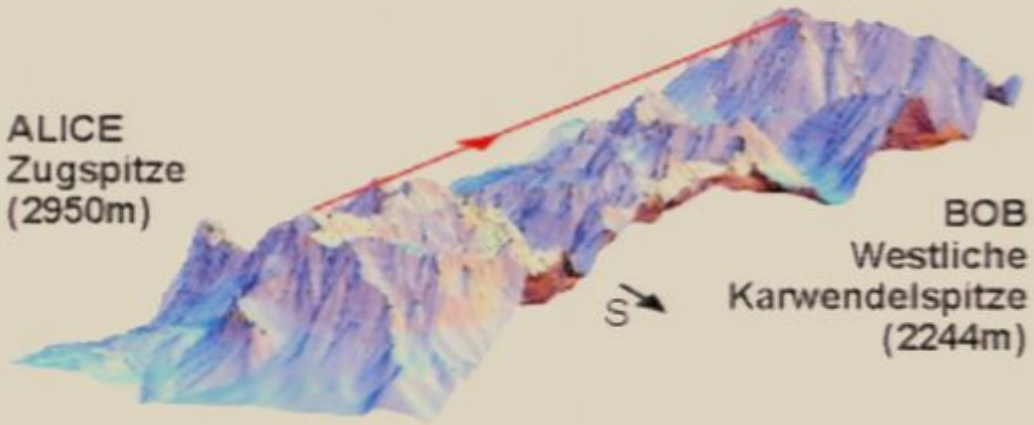
Quantum Key Distribution Implementations around the world



Quantum Key Distribution
Implementations around the world

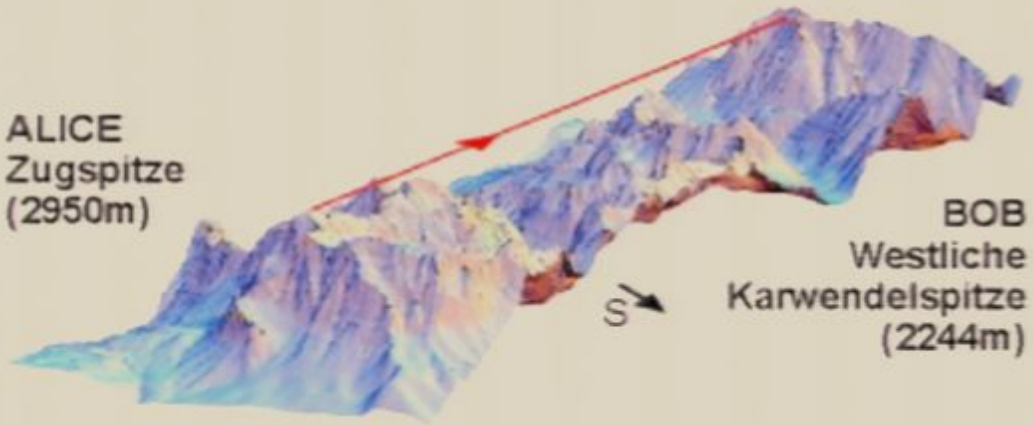


Quantum Key Distribution Implementations around the world

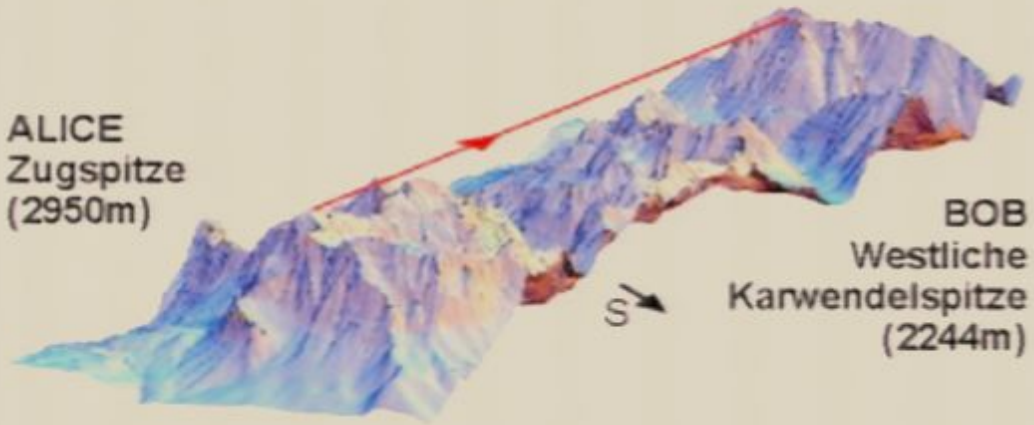


http://images.google.ca/imgres?imgurl=http://www.quantumlah.org/images/setup-79_800x600.jpg&imgrefurl=http://www.quantumlah.org/research/experimental&h=600&w=800&sz=128&hl=en&start=338&tbnid=vHhT5DopzpcYjM:&tbnh=106&tbnw=142&prev=/images%3Fq%3Dquant

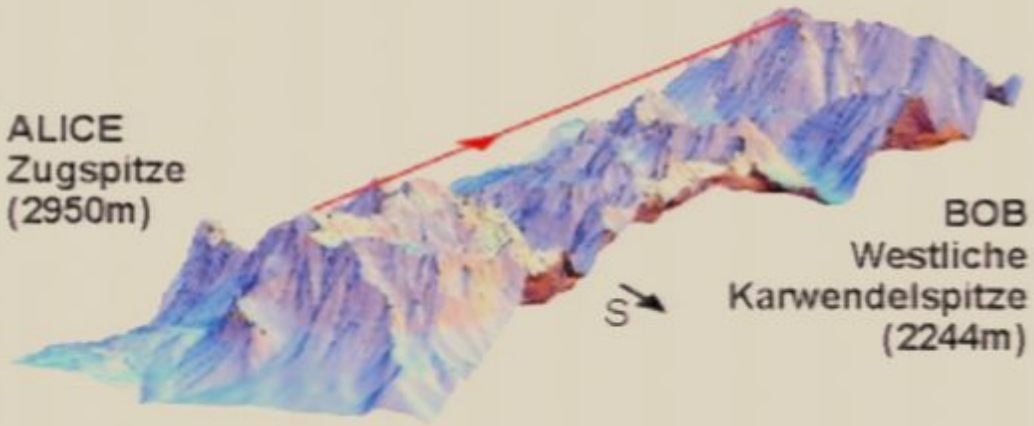
Quantum Key Distribution
Implementations around the world



Quantum Key Distribution Implementations around the world



Quantum Key Distribution Implementations around the world



Quantum Information Security

We must continually reassess the security of our existing information security infrastructure in light of the capabilities of quantum computers.

We can exploit the eavesdropper detection that is intrinsic to quantum systems in order to derive new "unconditionally secure" information security protocols. The security depends only on the laws of physics, and not on computational assumptions.

What technologies will be implemented and when?

Quantum random number generators: now.

Quantum key distribution: <10 years; some prototypes already available

Small scale quantum computers (e.g. needed for long distance quantum communication): medium term

Large scale quantum computers: medium-long term

Precise times are hard to predict since we are in the early stages and still trying a very broad range of approaches. Once we focus on technologies that show problem, expect progress to be very fast.

AN MIT ENTERPRISE

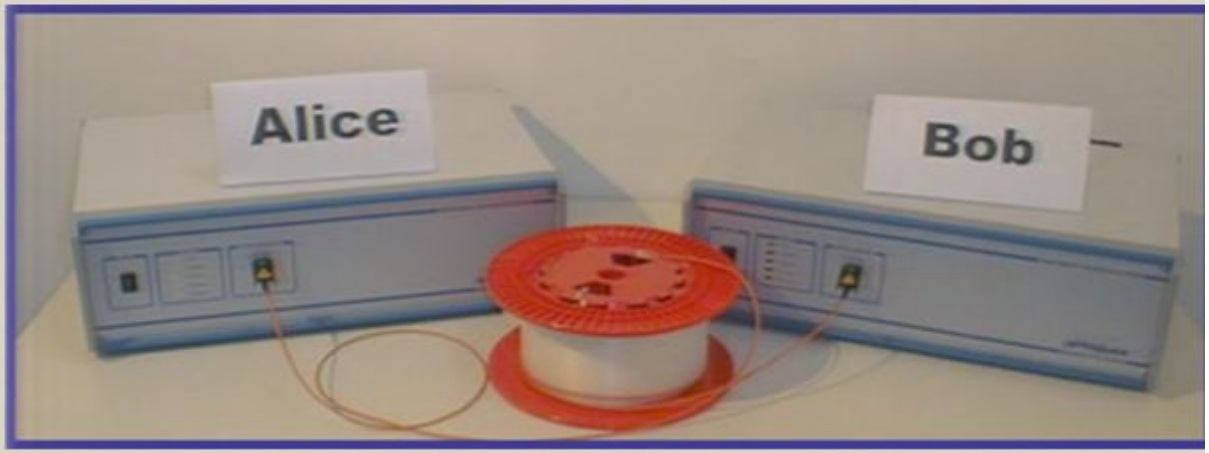
TECHNOLOGY REVIEW

Emerging Technologies and Their Impact

- Wireless Sensor Networks
- Injectable Tissue Engineering
- Nano Solar Cells
- Mechatronics
- Grid Computing
- Molecular Imaging
- Nanoimprint Lithography
- Software Assurance
- Glycomics
- **Quantum Cryptography**

id Quantique

A quantum leap for cryptography



MagiQ™

Quantum Information Solutions for the Real World.

REDHERRING

we made the cut!

DEMO | 2003

[demonstrator]

Founded in 1999, MagiQ™ Technologies combines science, business, and engineering expertise with a commitment to commercialize advances in quantum physics. Currently, MagiQ is developing real-world security implementations of several field-tested quantum information solutions. In addition, MagiQ continues to build its portfolio of intellectual property around quantum information processing.

Conclusions

- Quantum mechanics is for real
- Quantum mechanics redefines information and information processing
- Large scale quantum information processors seems possible, though technologically very challenging to realize
- Serious prototypes for quantum communication and cryptography already exist
- Some of the basics accessible to HS students