KØBENHAVNS UNIVERSITET

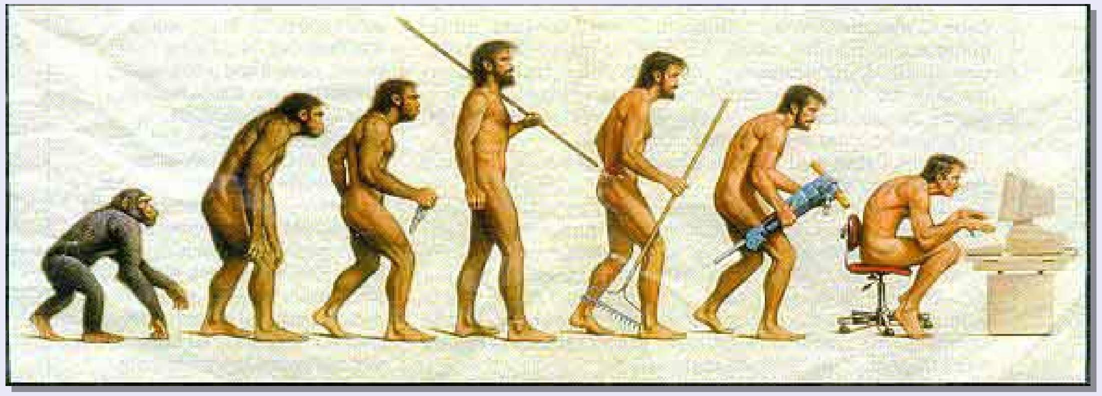
Quantum Information and Computation

Michael J. Kastoryano
Niels Bohr International Academy

Contents

Philosophical observations

Physics differs from other sciences



In biology there are Principles

In physics there are Laws

Both the Laws and the Theories were incorrect in Classical Physics.

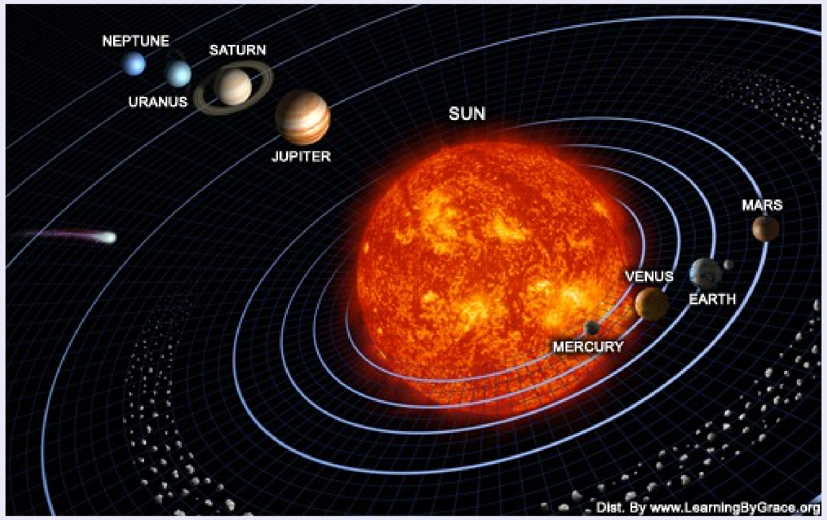
Classical Physics (ca. 1900)

Nature's cookbook: classical physics

Theory

Forces

+

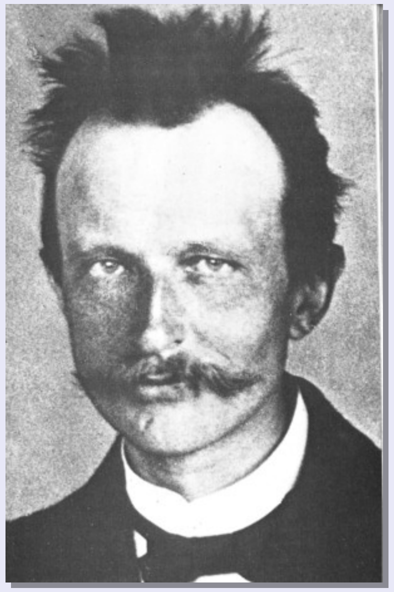


Newtonian mechanics

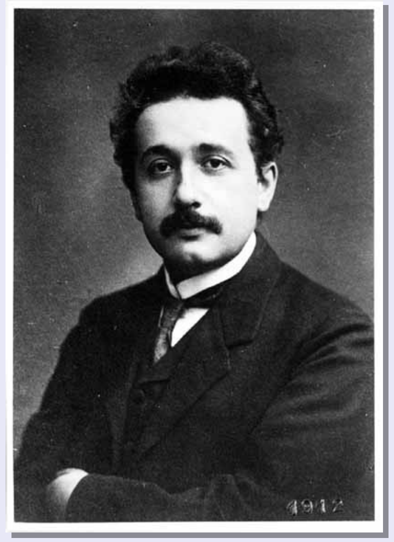
Newton's gravity

Maxwell's electromagnitism

Quantum Mechanics (1900-13)



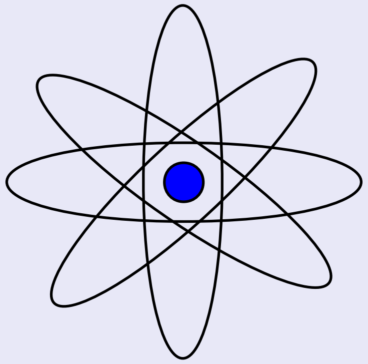
Planck's energy quantum



Einstein's photoelectric effect

Bohr's atomic model:

Not quite right



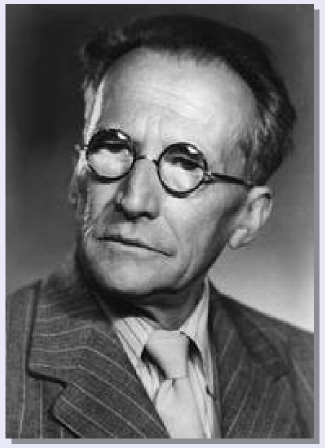
Quantum Mechanics:
"describing the internal mechanics of atoms"

Quantum Theory (1925-30)

Particle Wave duality (DeBroglie)

Heisenberg uncertainty relations

Pauli's exclusion principle



Probabilistic interpretation
of the wavefunction

But there is more:
measurement problem and entanglement

Philosophical disagreement

Gott würfelt nicht

Albert Einstein

Doch!

Niels Bohr

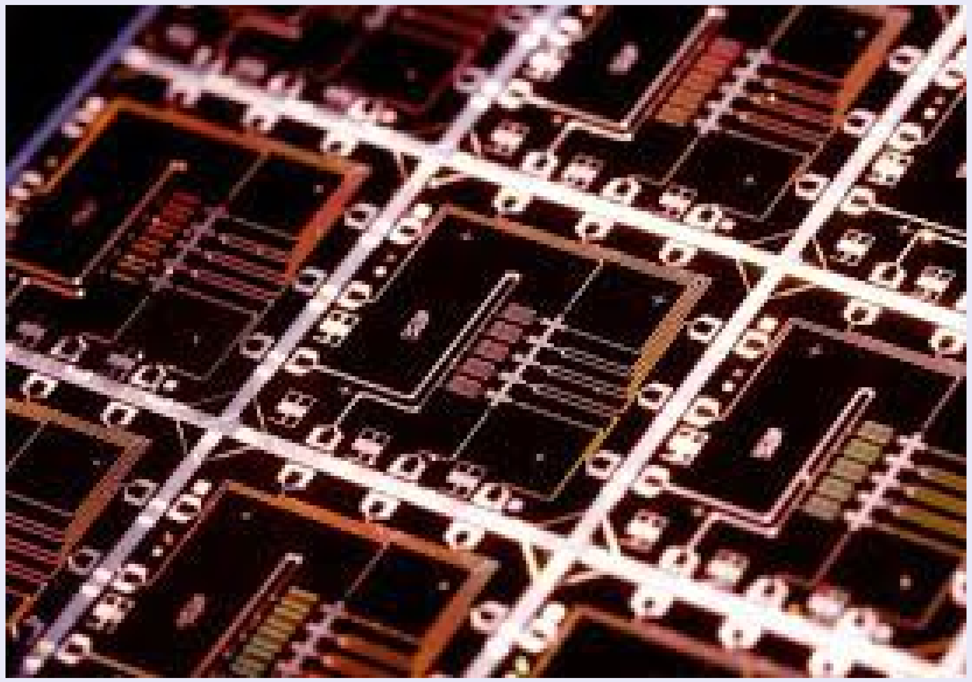
3 quantum revolutions

First quantum revolution: quantum mechanics (~1910)
The first cracks in the classical theory were perceivable. QM filled the cracks

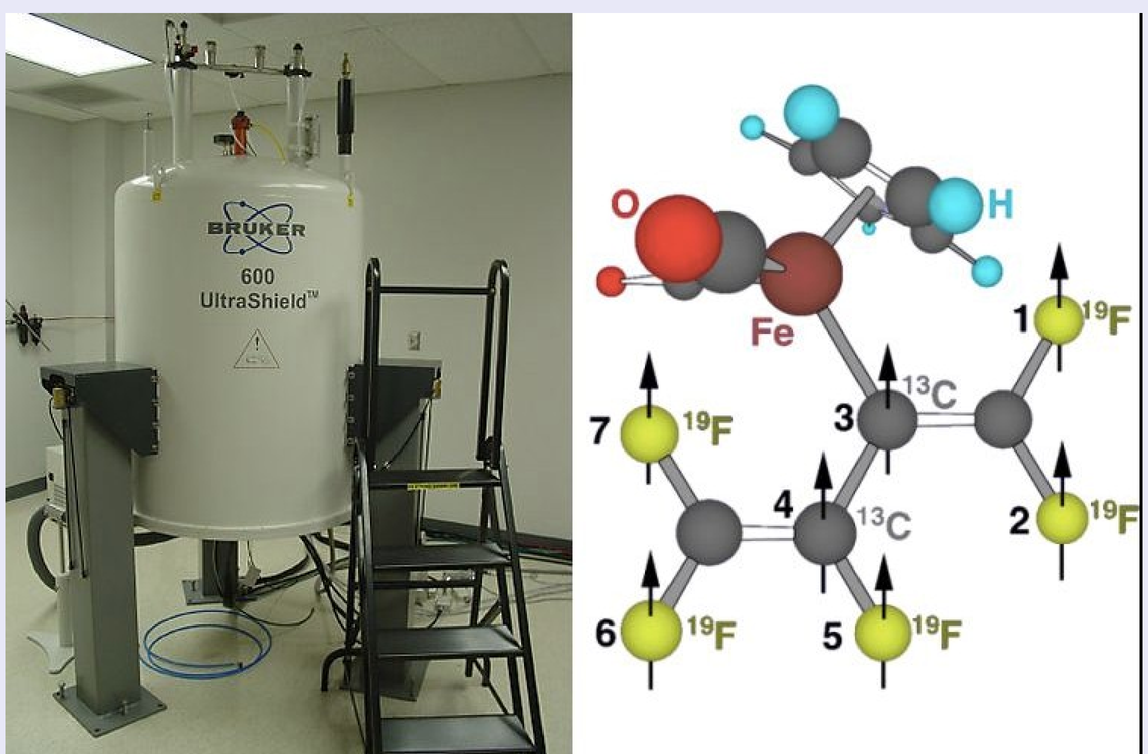
Second quantum revolution: quantum theory (~1930)
All experiments on microscopic objects could be explained again with the new complete framework.

Third quantum revolution: quantum information theory (~1990)
Microscopic objects can now be manipulated one by one. We are quantum engineers.

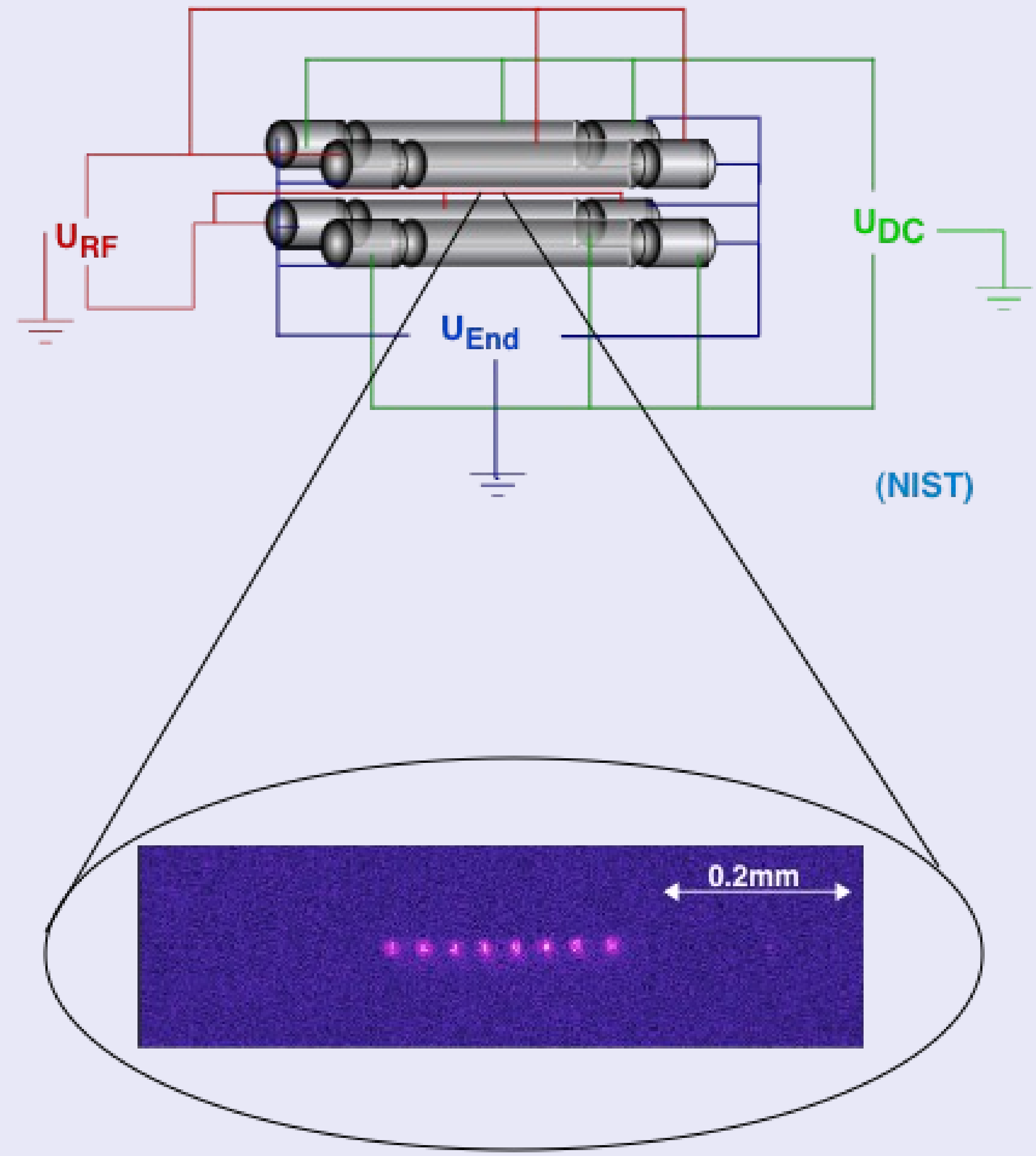
Controlled quantum systems



Superconducting circuit

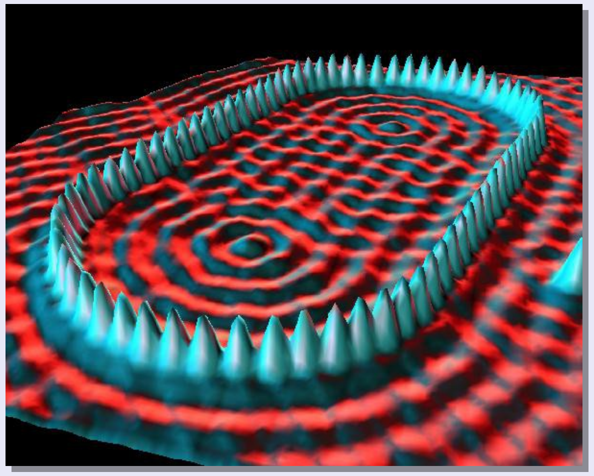


NMR



Ions in a trap

What is Quantum Information?



Quantum Mechanics

Computer Science

Information Theory

Quantum Information

Quantum theory is strange
Quantum logic is different

Bohr and Einstein: many discussions on the meaning of the new theory. **Philosophy**

Today, we can see how individual atoms behave. Quantum mechanics is reality. **Physics**

Can we make use of these strange properties?

Quantum information: use the weird logic to build new computers. **Technology**

Particles and waves

Wave

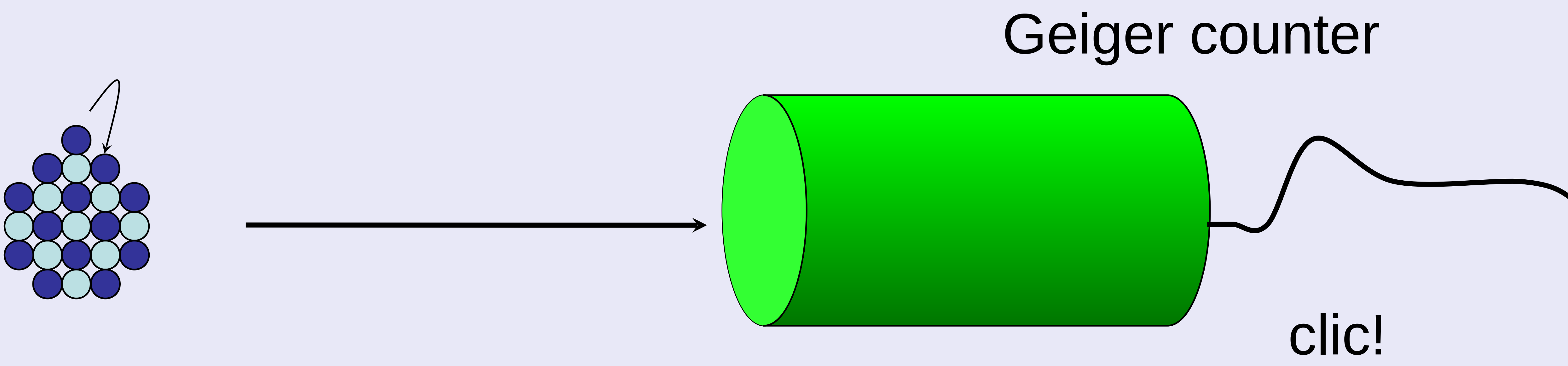
Particles

Fundamentally different behavior!

Light is also a particle

Radioactivity: atomic nuclei decay and emit radiation

γ-radiation is light of a very high frequency



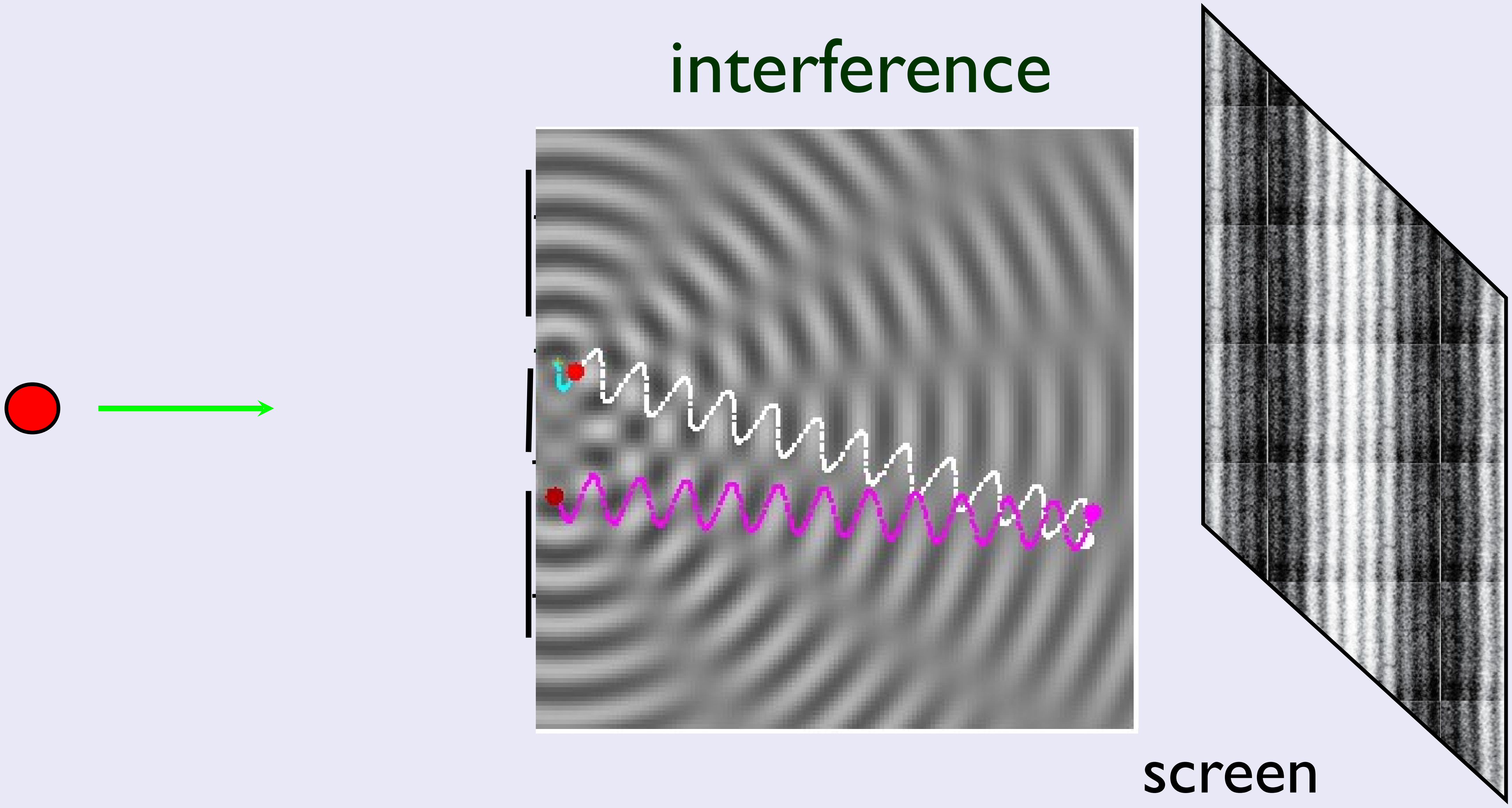
Explanation (Einstein/Planck): light is a particle; photons

Light is both particle and wave at the same time

Particle-wave duality

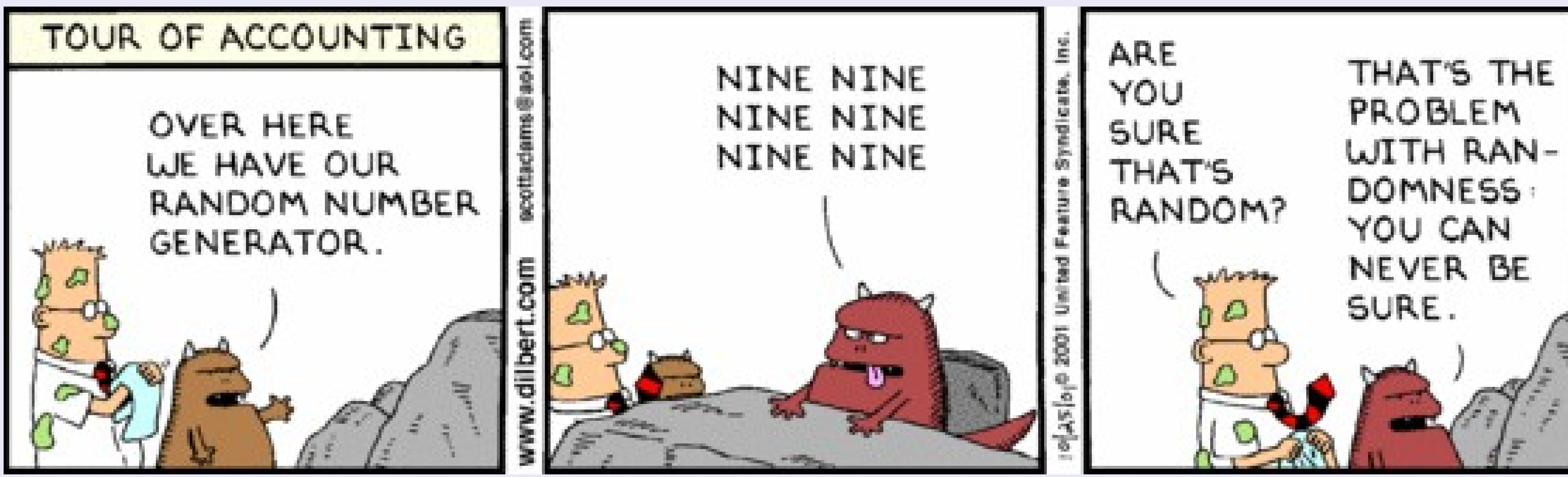
Quantum theory: everything is simultaneously wave and particle

Ex: double slit experiment with electrons



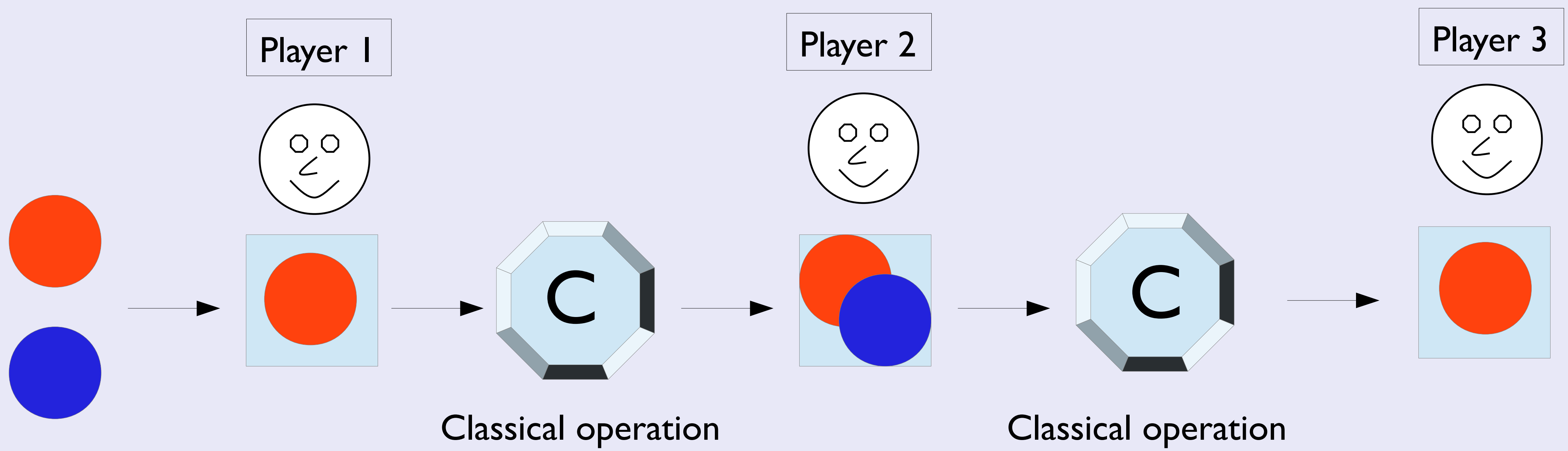
There exit two types of randomness!

Classical randomness = lack of knowledge of the observer



Quantum randomness = intrinsic

Classical vs Quantum probability game



0) Start with some mixture of red and black balls

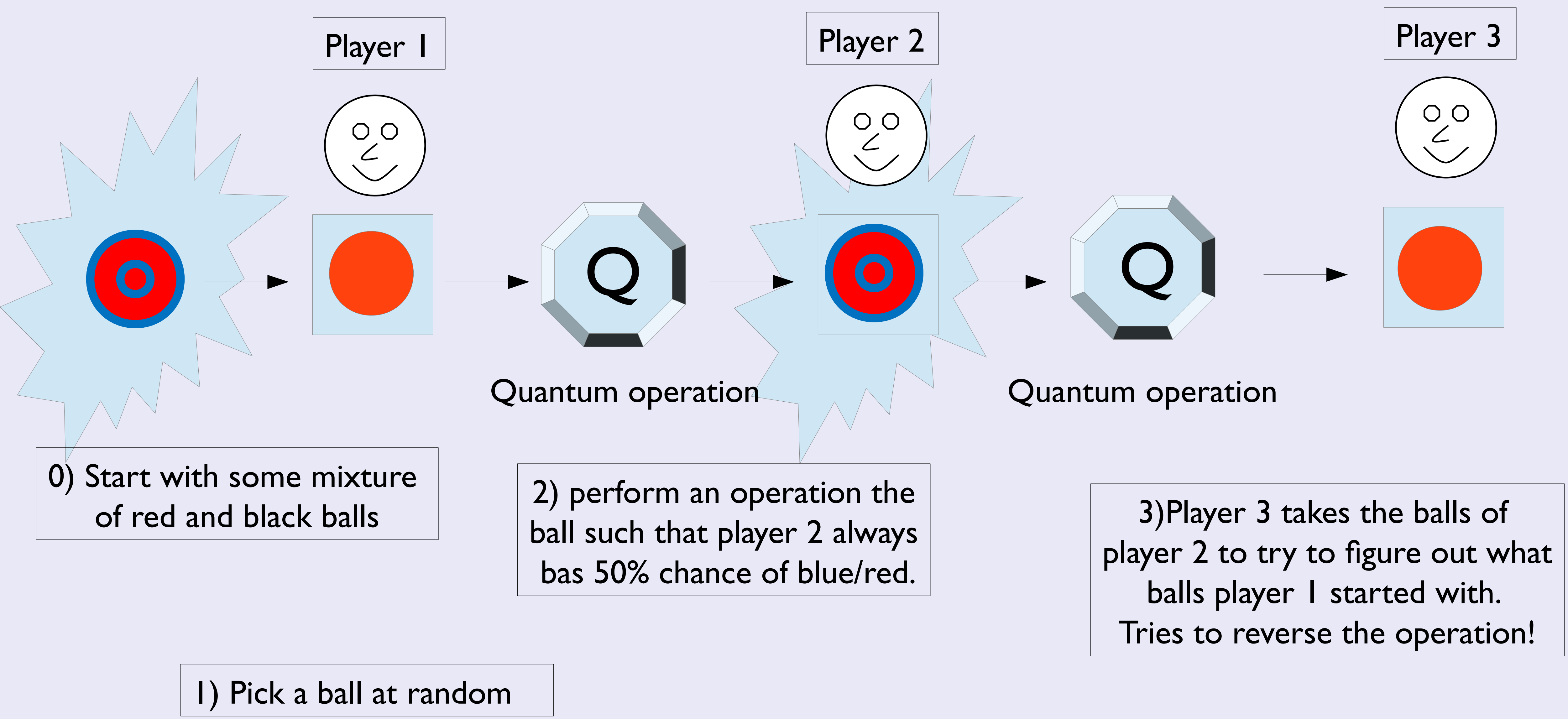
2) perform an operation the ball such that player 2 always has 50% chance of blue/red.

3)Player 3 takes the balls of player 2 to try to figure out what balls player 1 started with.
Tries to reverse the operation!

1) Pick a ball at random

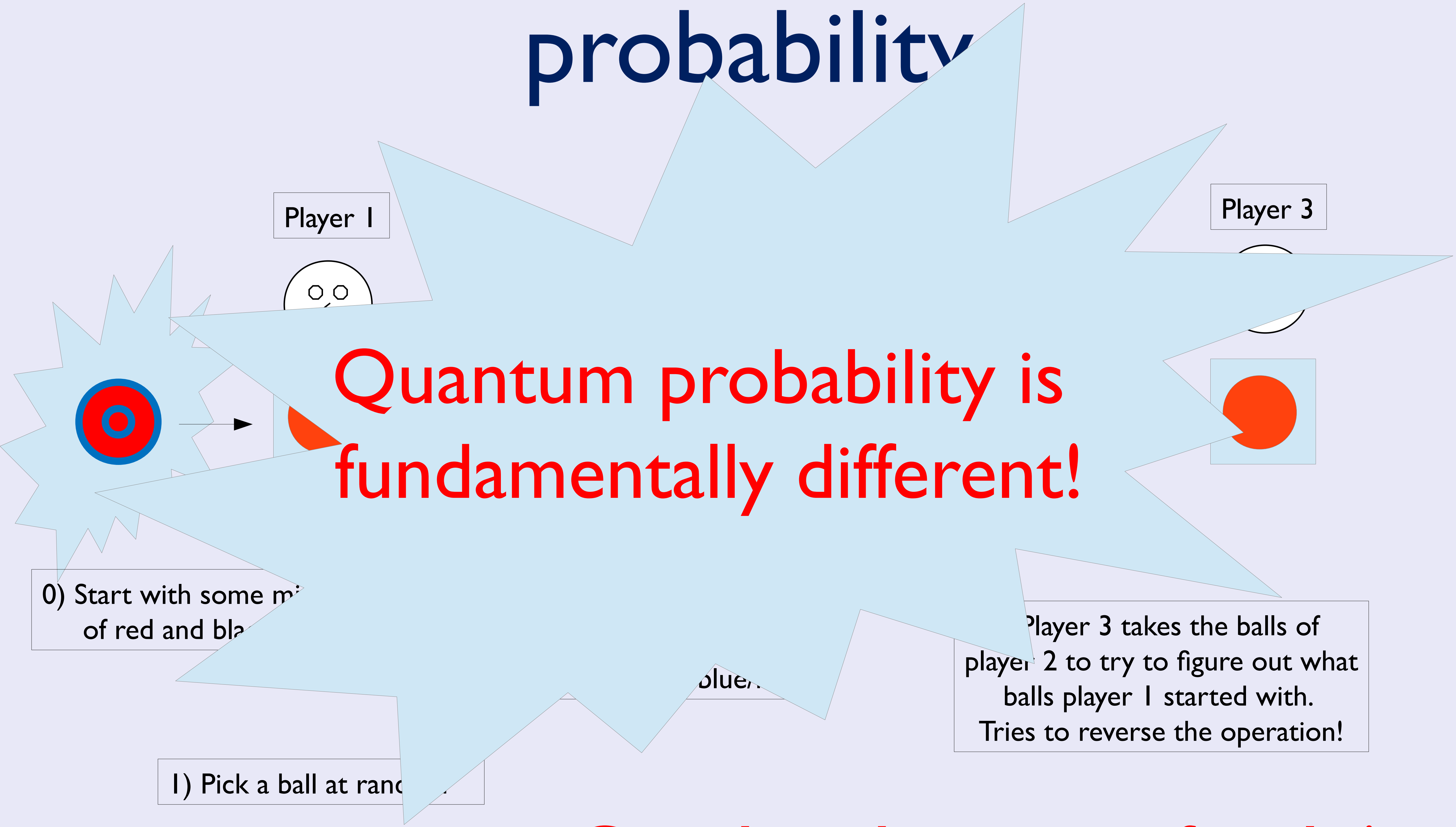
Impossible!

Classical vs Quantum probability



Can be done perfectly!

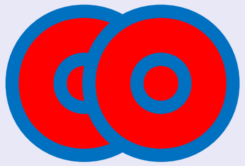
Classical vs Quantum probability



Can be done perfectly!

Quantum vs. Classical randomness

Is both red and blue at the same time: no lack of knowledge

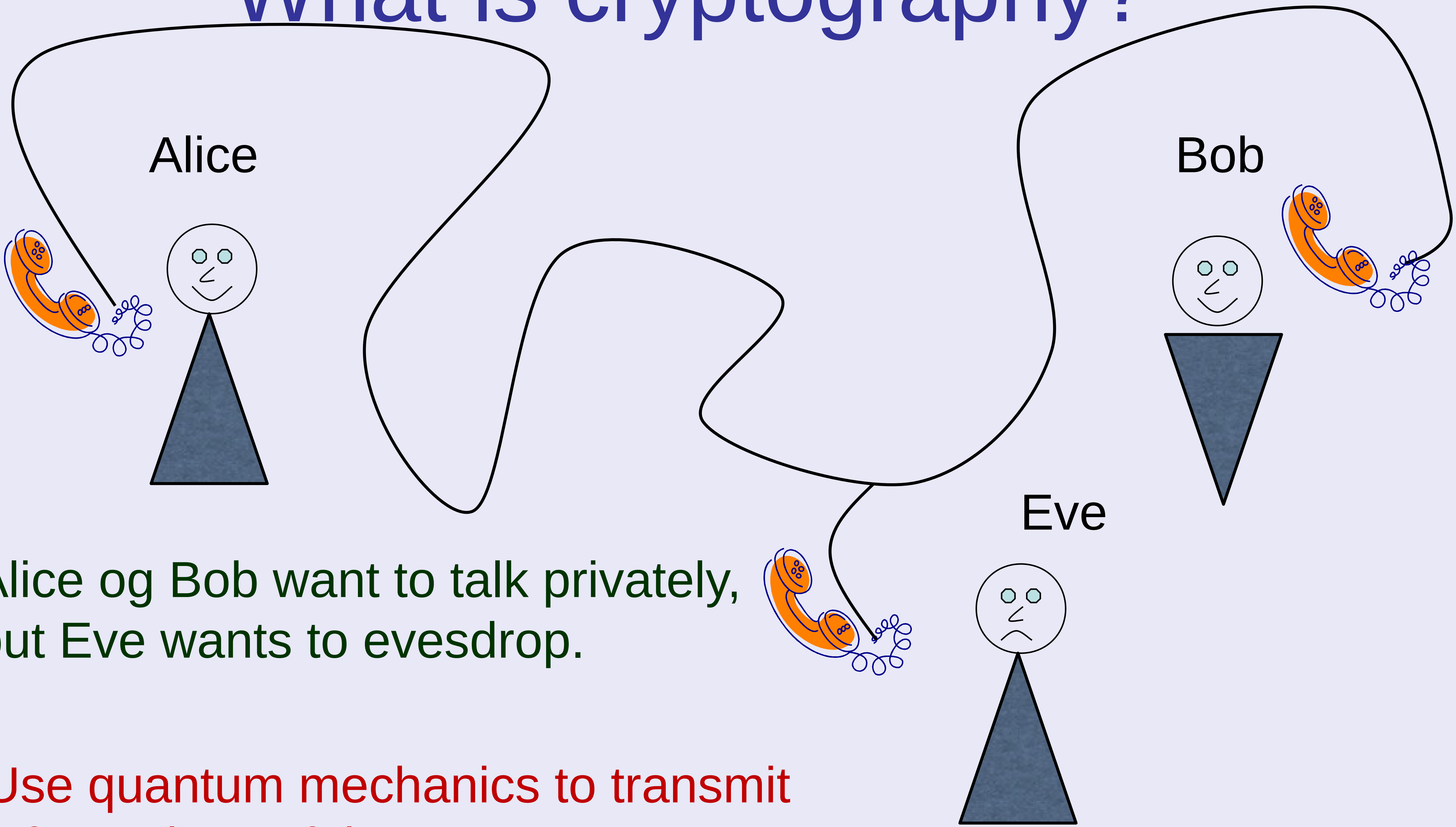


Entangled pair: both blue and both red at the same time!

Entanglement is what makes quantum computation possible!

Quantum cryptography

What is cryptography?



Alice og Bob want to talk privately, but Eve wants to evesdrop.

Use quantum mechanics to transmit information safely.

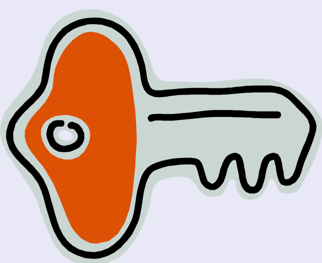
Encrypt a message

Message

Hello world

Encrypted message

Jr;;p ept;f



Take every letter, and replace it with its right neighbor on the keyboard

Goal of a cryptosystem is to find a good encryption scheme and to protect the key.

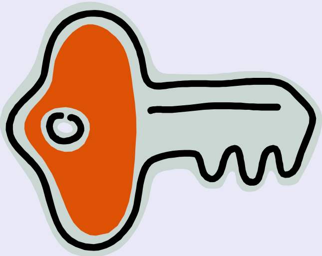
It can be difficult to protect against evesdroppers!

Realistic situation

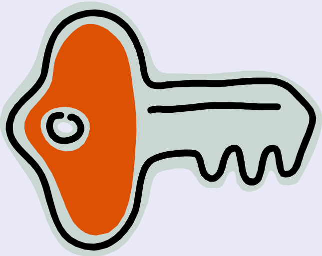
Netbanking

How can you get a key without having to go down to the bank to fetch it?

Solution: use algorithmic complexity and two secret keys.



Public key for encryption



Private key for decryption

Example: RSA

Take two prime numbers

p1= 11125651

p2= 3455591

p12=p1*p2=38445699464741

It is difficult to find p_1 og p_2, if you only know p_{12}.

Protocol:

1. You have a large prime (p_1) on your computer
2. The bank knows your prime (p_1) and multiplies it with another unkown prime (p_2)
3. The product (p_{12}) is the public key, that the bank uses to ecrypt the message it send to you.

The message can only be read if you have (p_1)

Cryptosystem is secure if factoring is difficult!

Example: RSA

Take two prime numbers

p1= 11125651

p2= 3455591

p12=p1*p2=38445699464741

It is difficult to find p_1 og p_2, if you only know p_{12}

Protocol:

1. You ... a l ...) ... your computer
2. Th ...) and multiplies li ... 2)
3. ... y, that the ... the message it send to you

The message can only be read if you have (p_1)

Quantum computers can factor efficiently!

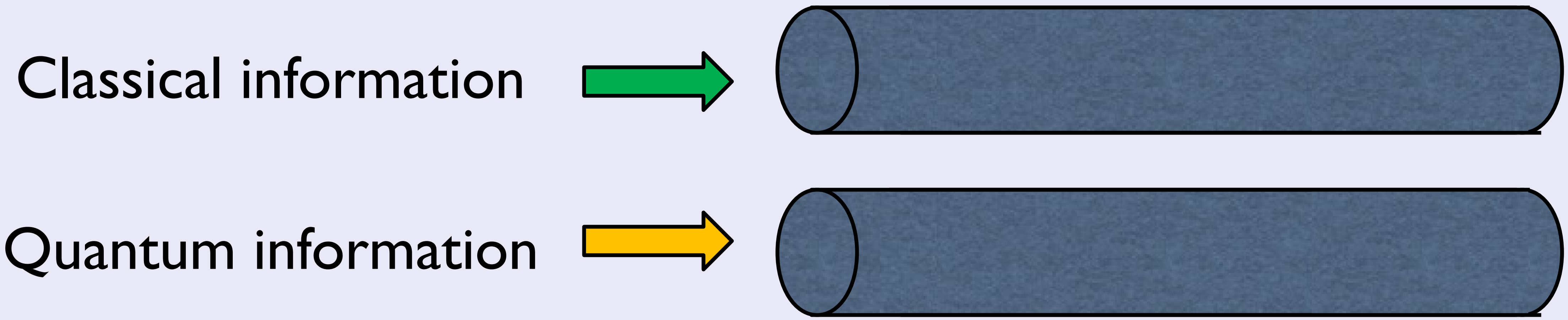
Cryptosystem is secure if factoring is difficult!

Quantum algorithms

New possibilities:

- Database search $\sqrt{N} \ll N$
- Factoring large numbers ⟹ Can crack RSA
- Quantum cryptography is necessary
- Simulate quantum systems

Quantum solution: BB84



Idea: Send quantum information through a quantum channel, and use a classical channel to verify if there was an evesdroper.

If there was an evesdroper ⟹ Message cannot be used as a private key

If there was no evesdroper ⟹ Message can be used as a private key.

Quantum solution: BB84

Classical information

Quantum information

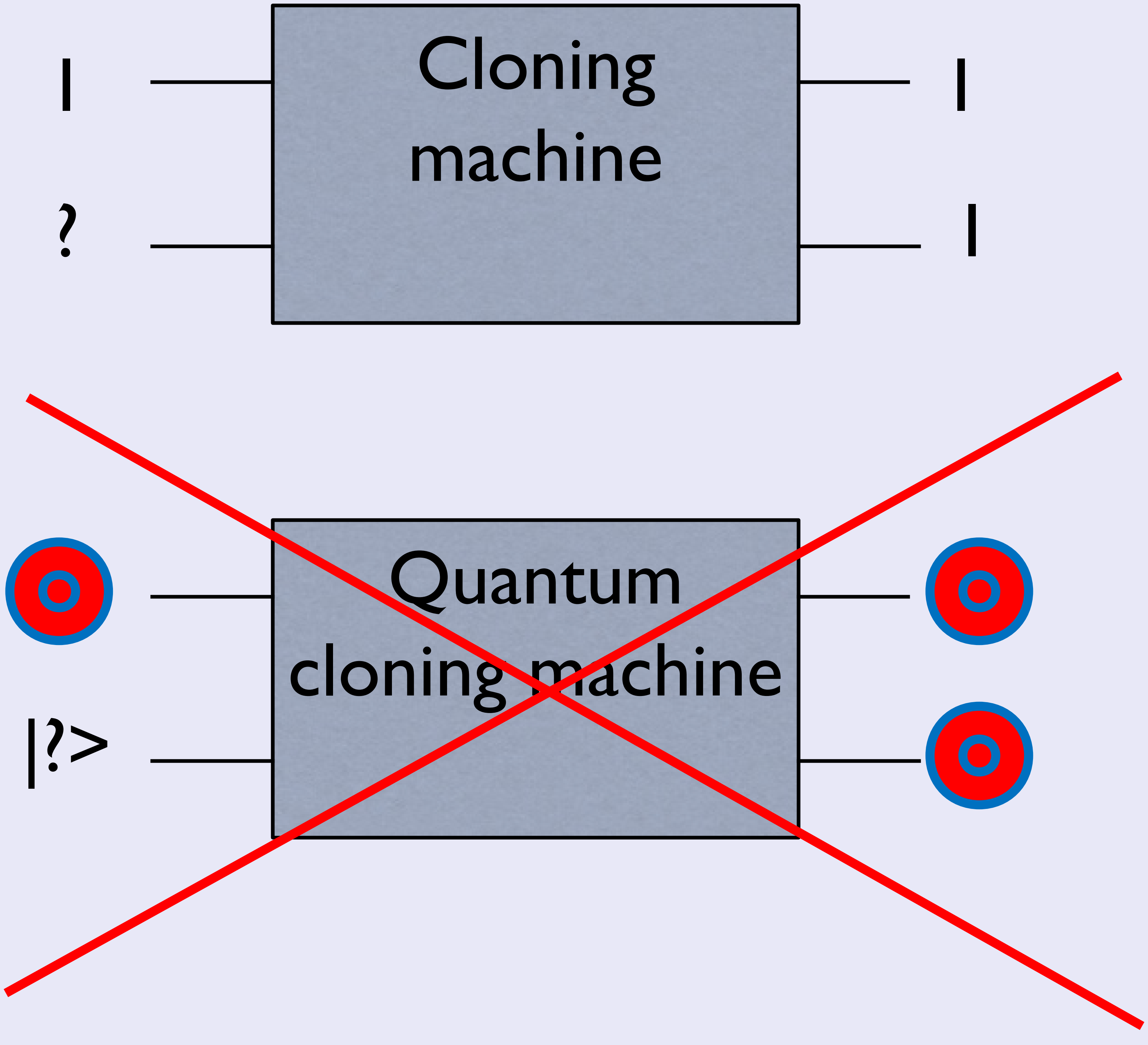
Idea: Send quantum information th… ugh a quantum channel, ar… use a … ann… to verify if there was ar…

Works because of No-cloning Theorem

If there was ar… …essag… cannot be used as a private key

If there was no evesdroper ⟹ Message can be used as a private key.

No-cloning principle



In practice

id Quantique
A Quantum Leap For Cryptography

MagiQ

SmartQuantum

Up to 100km distance

Was used for local elections in Geneva

Used for online casinos $$$$$$

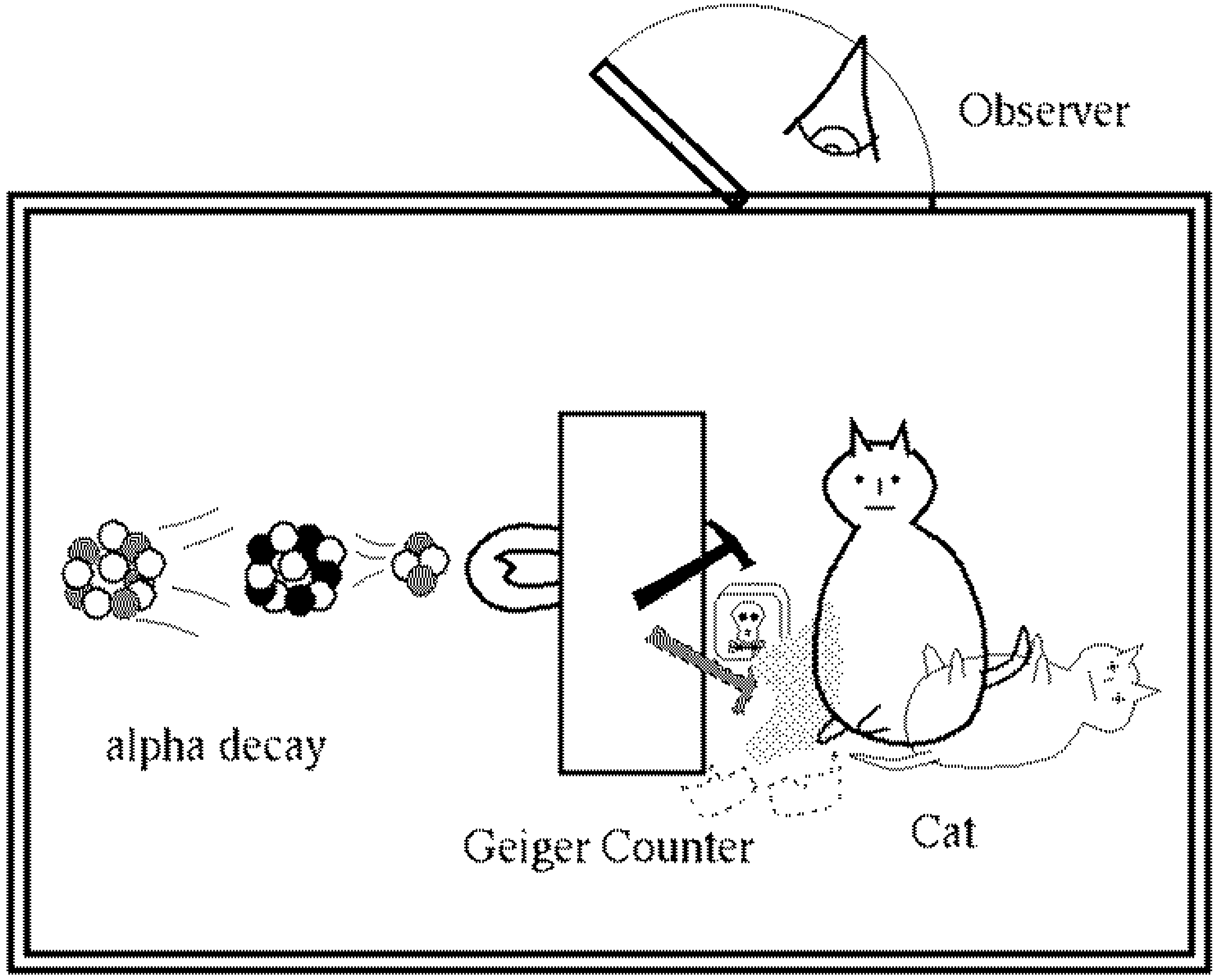
Conclusion (1)

Quantum mechanics is strange – things can be at two places at the same time.

We can use this weirdness for something useful

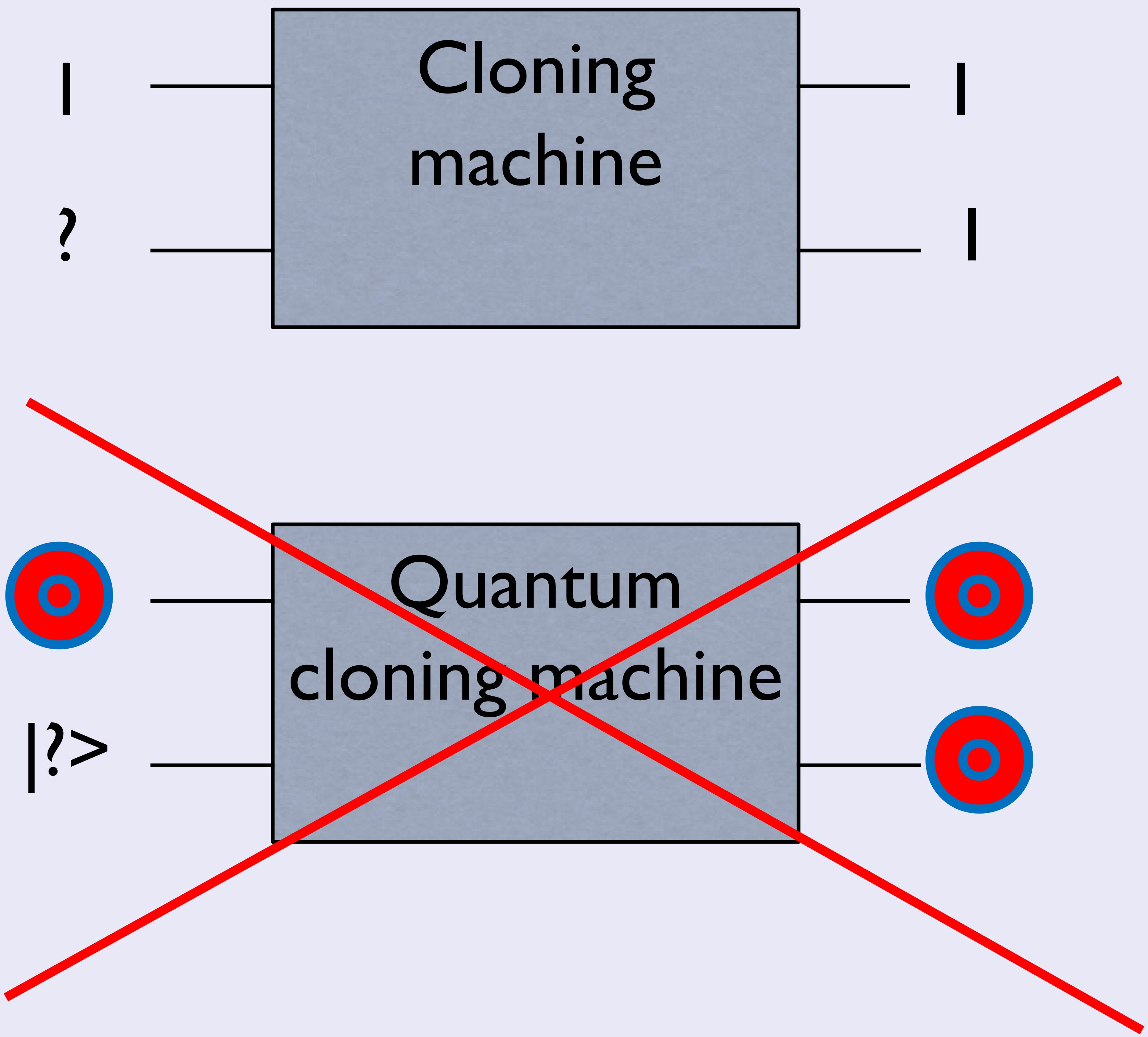
- Quantum cryptography

What else can we use it for?

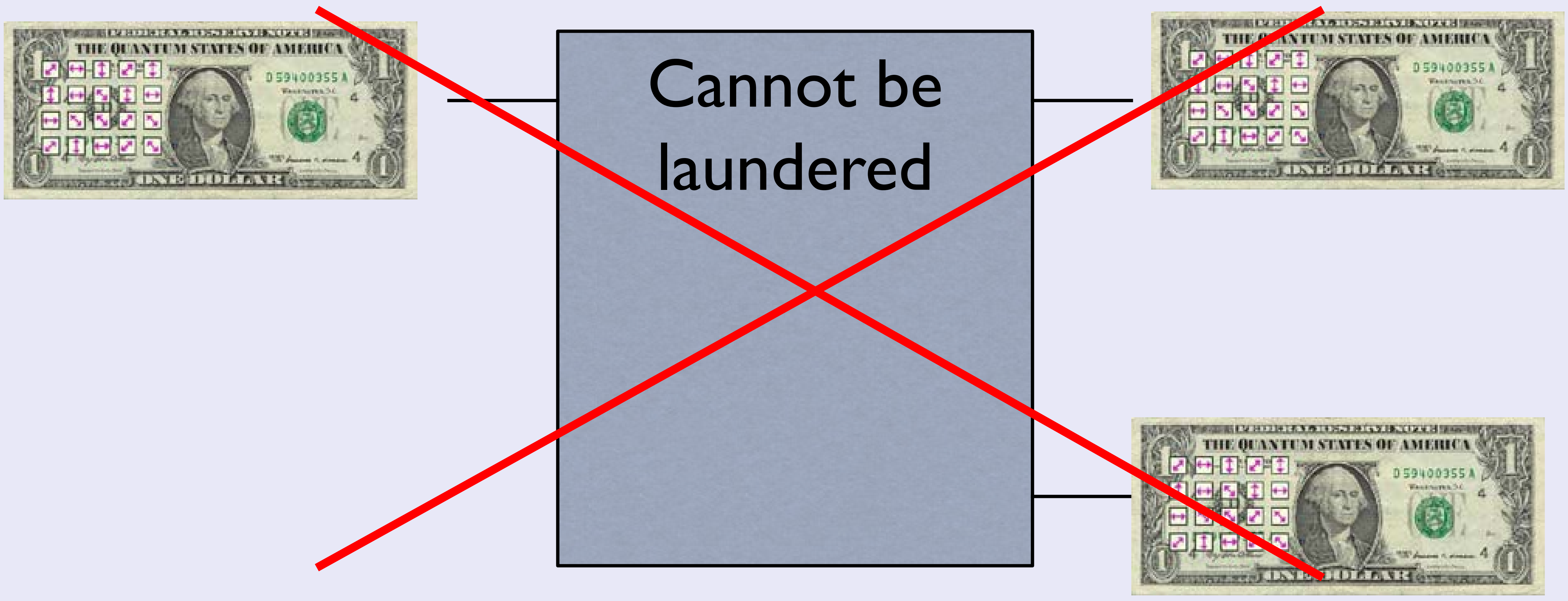

Observer
alpha decay
Geiger Counter
Cat

Contents

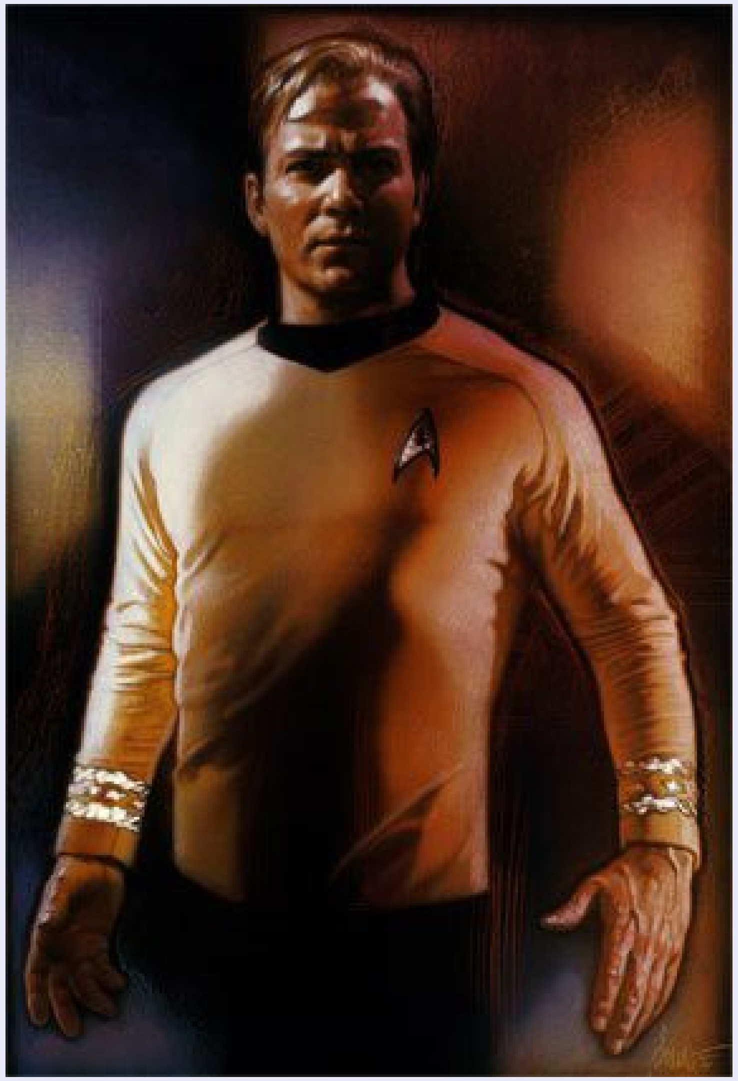
No-cloning principle

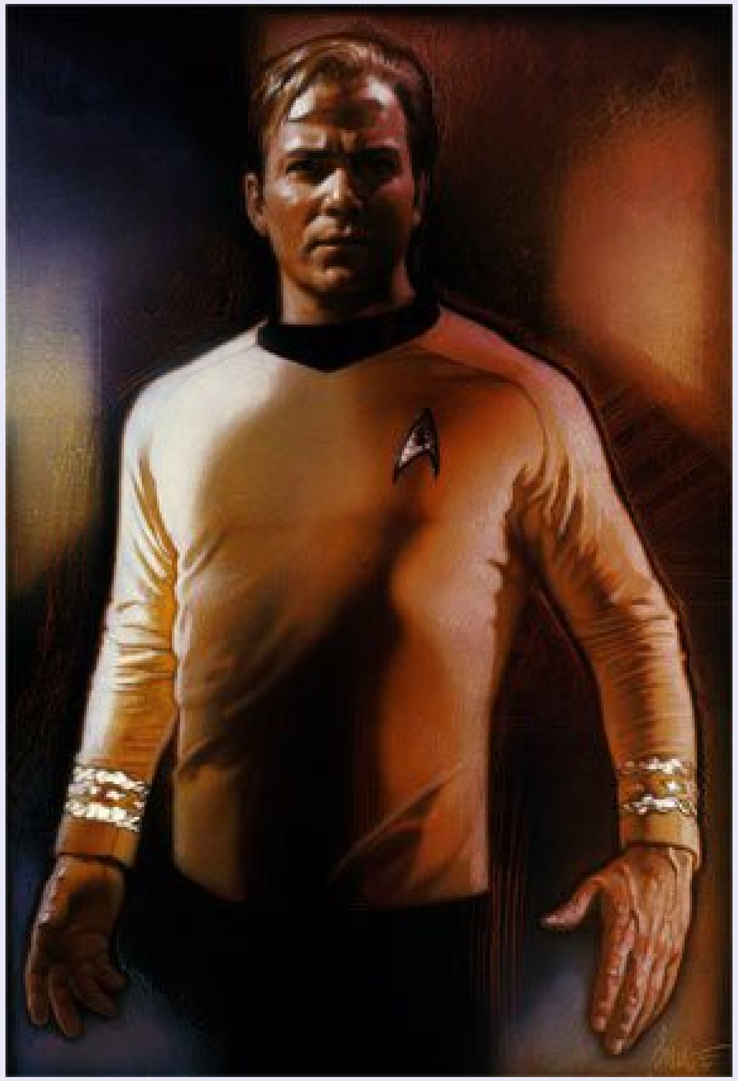


Quantum money?



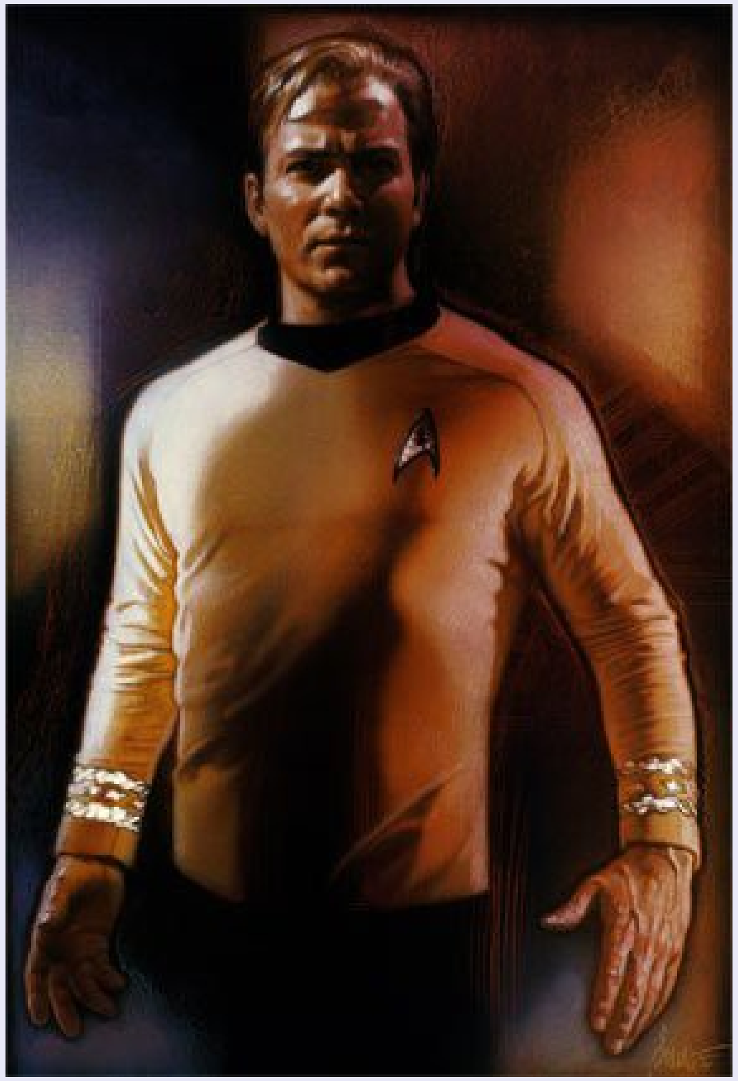
Teleportation





Teleport: copy information and rebuild it elsewhere

Teleportation

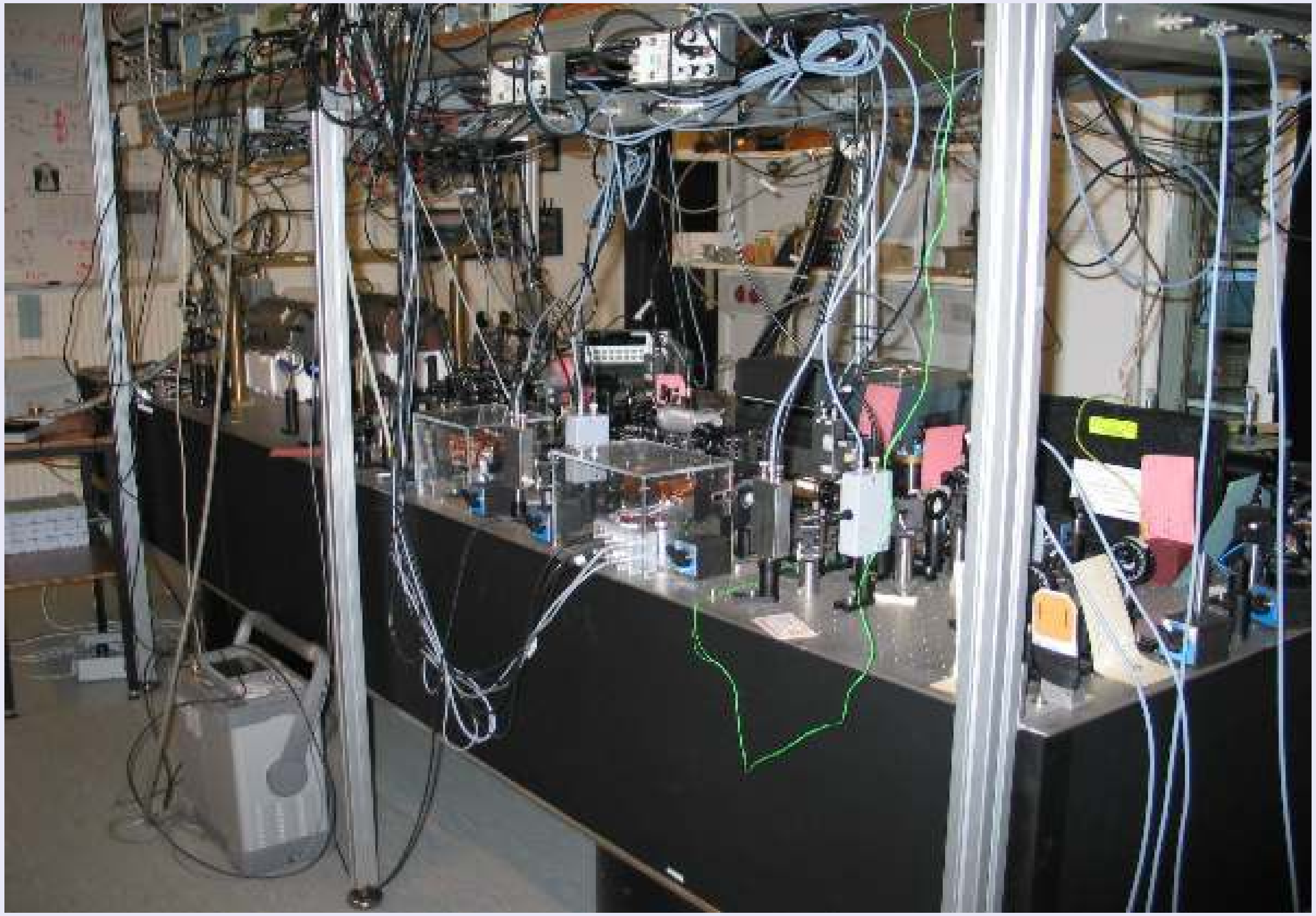


Teleport: copy information and rebuild it elsewhere

A good teleporter

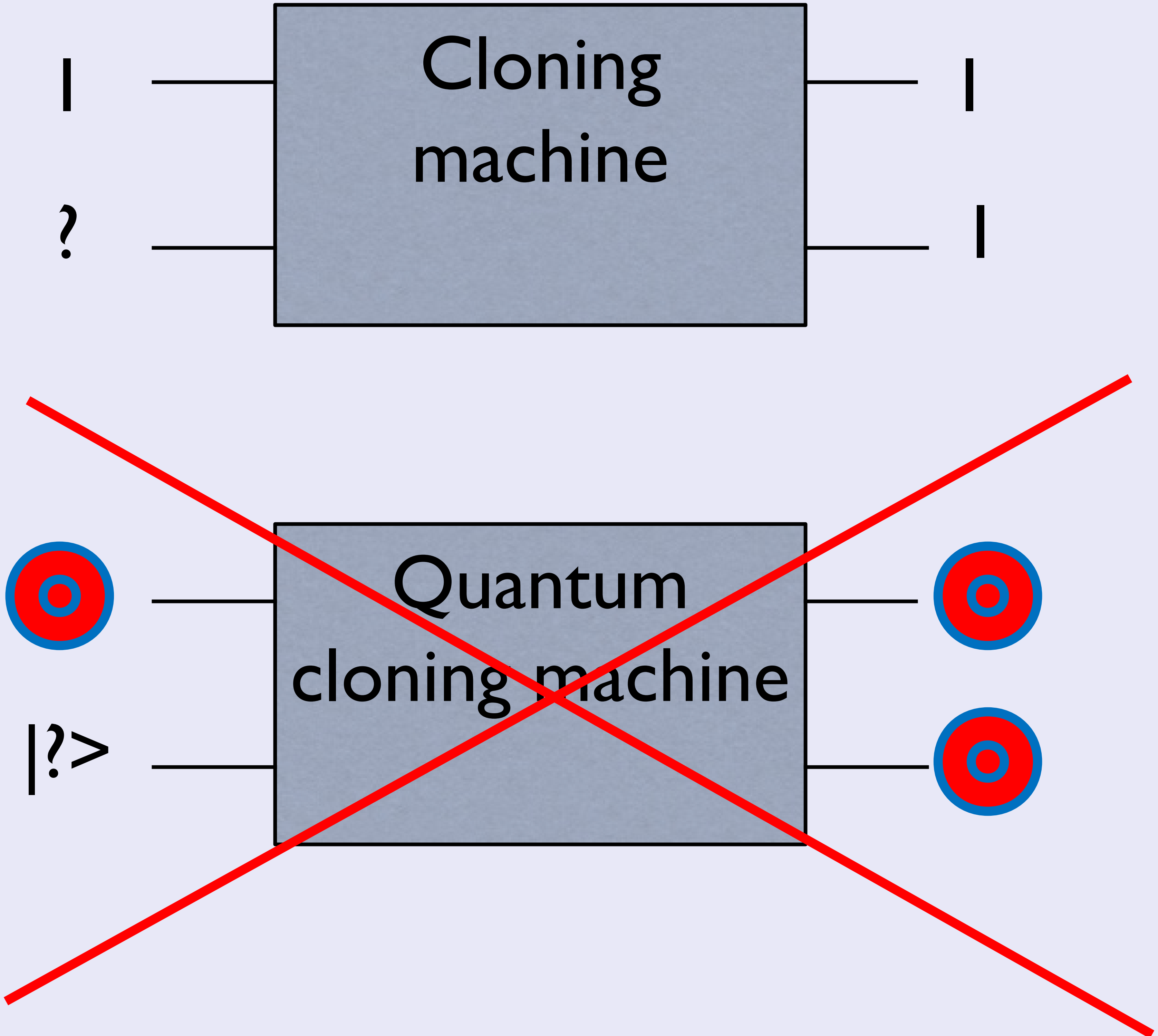
Telefax: reads the information on a piece of paper, copies it, sends the information to the receiver, and copies it down there.

Another teleporter



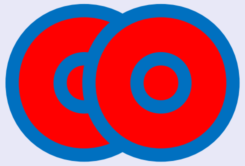
Able to teleport quantum information

But no-cloning principle



Quantum vs. Classical randomness

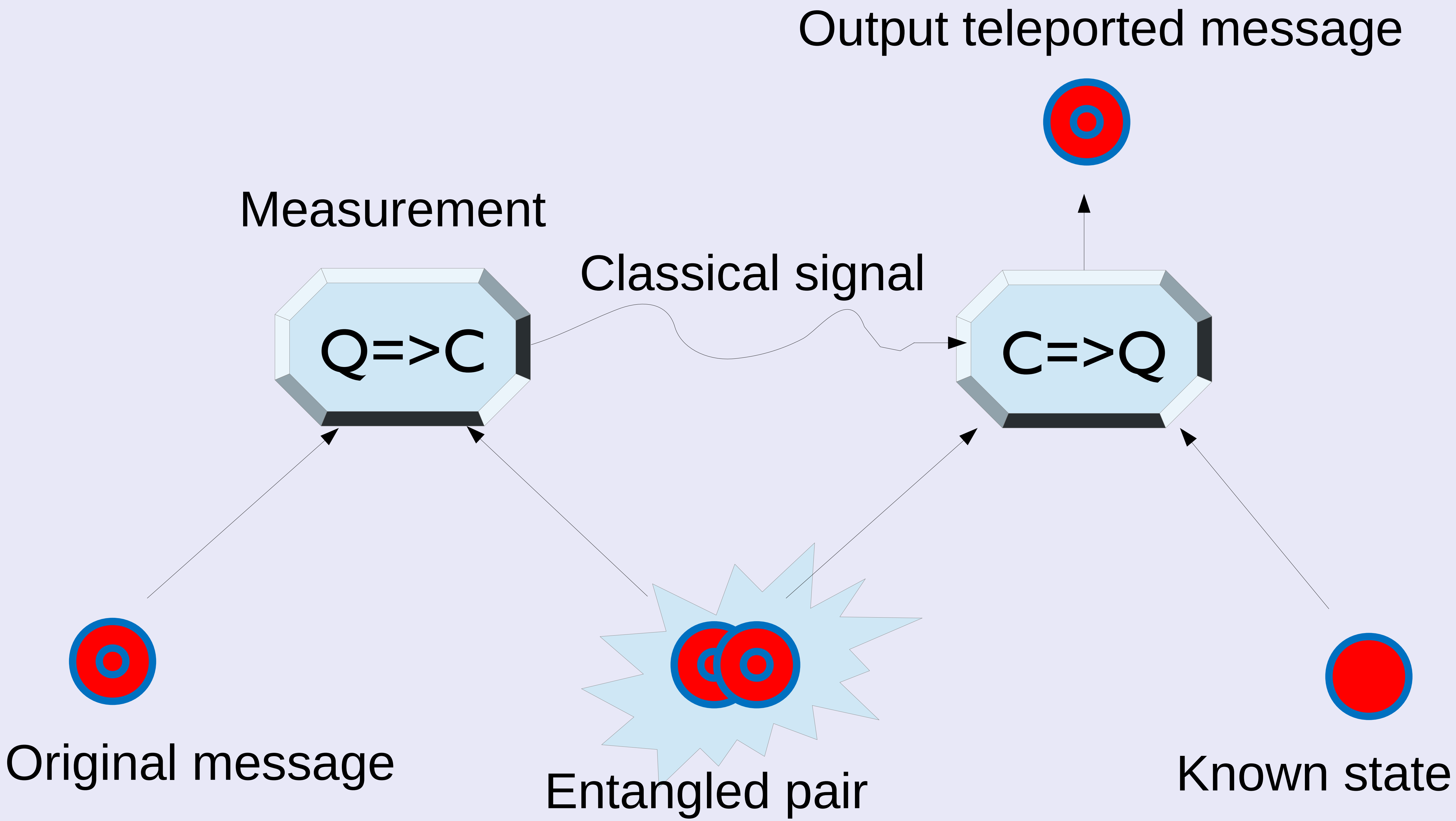
Is both red and blue at the same time: no lack of knowledge



Entangled pair: both blue and both red at the same time!

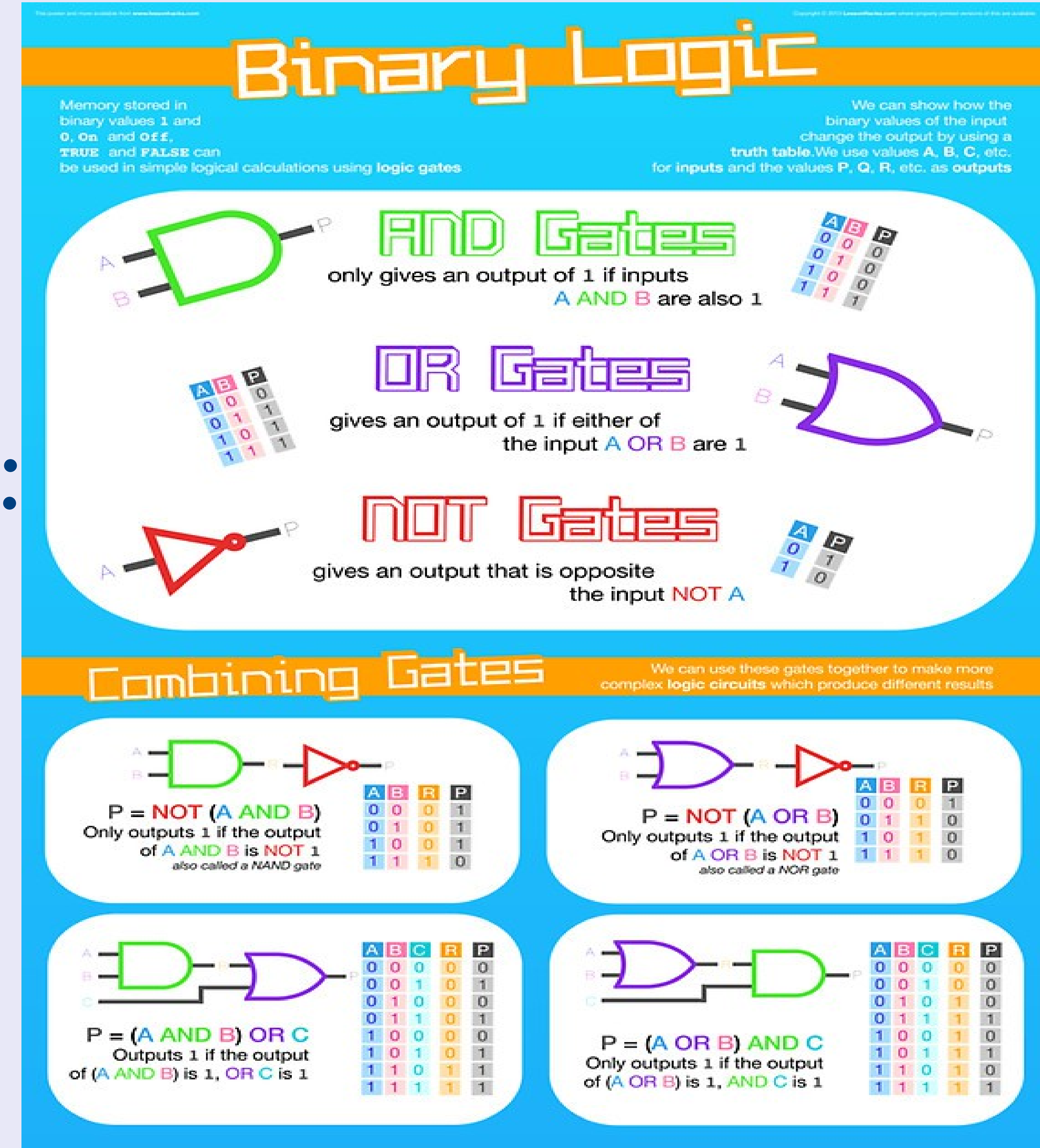
Entanglement is what makes quantum computation possible!

Solution: Entanglement

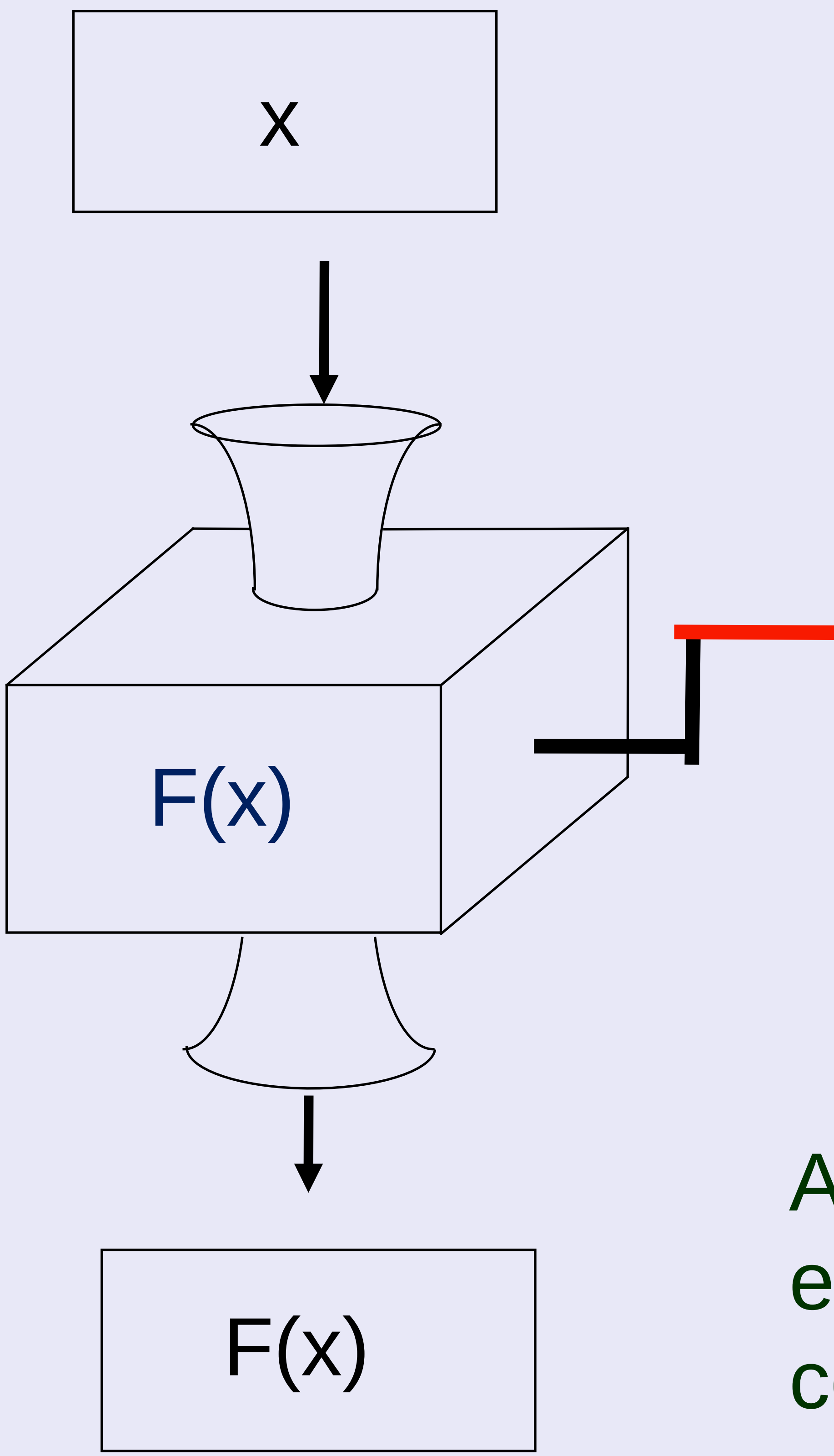


Next level:
Quantum computers

Classical computers: Binary Logic



Classical computer



Efficiency:

x= "00101110100111001" Length N

How long does it take for the function F(x) to be calculated?

~N^k times ⟹ eff cient

~Exp(N) times ⟹ ineff cient

Are quantum computers more eff cient than classical computers?

Yes!

Church Turing Thesis:

A problem that is hard on one computer will be hard on all computers!

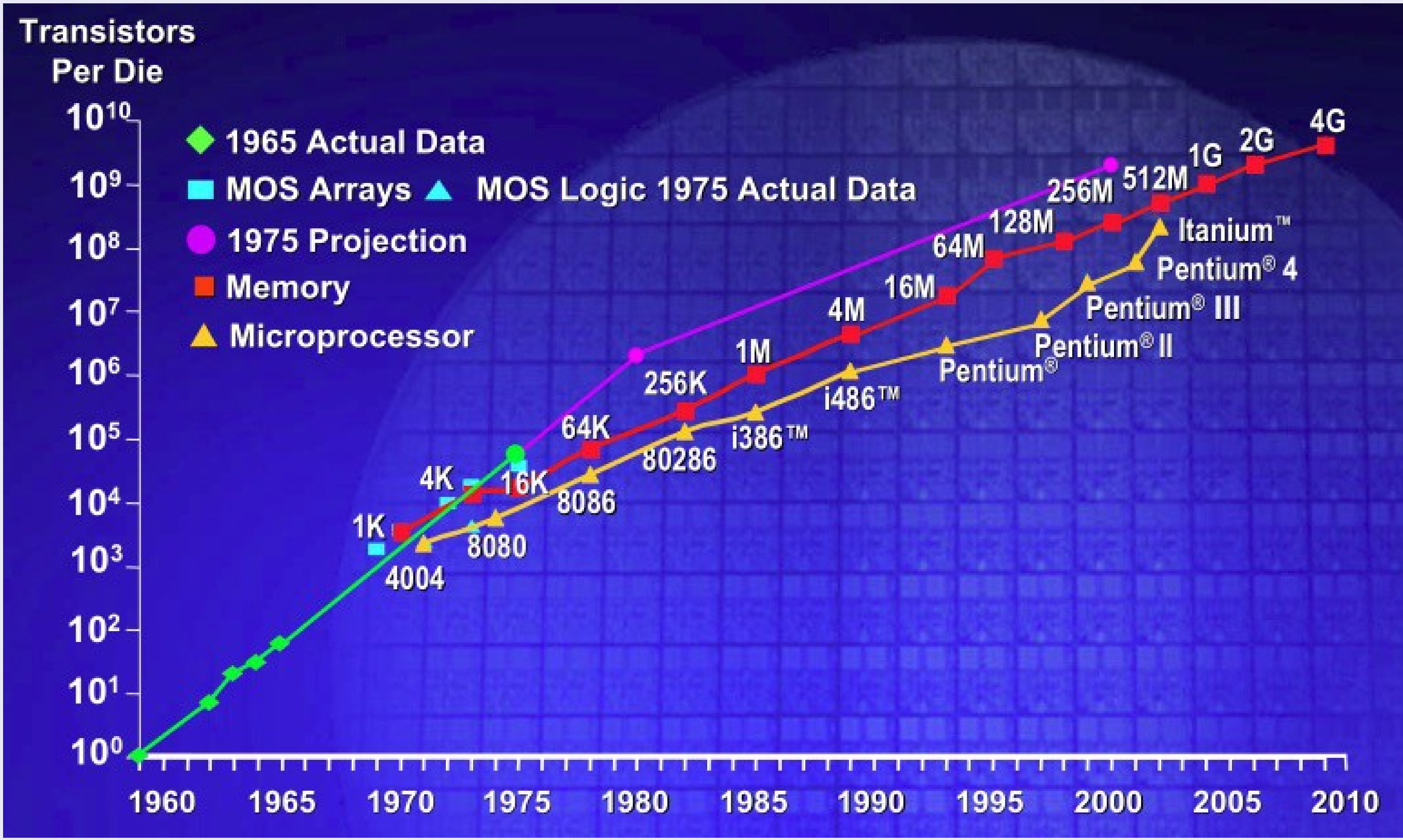
Church Turing Thesis:

A pro d

on e

Quantum computers
Violate the Church-Turing thesis!

Moore’s Law



Transistors Per Die
1965 Actual Data
MOS Arrays
MOS Logic 1975 Actual Data
1975 Projection
Memory
Microprocessor
1K
4K
16K
64K
256K
1M
4M
16M
64M
128M
256M
512M
1G
2G
4G
4004
8080
8086
80286
i386™
i486™
Pentium®
Pentium® II
Pentium® III
Pentium® 4
Itanium™
1960
1965
1970
1975
1980
1985
1990
1995
2000
2005
2010

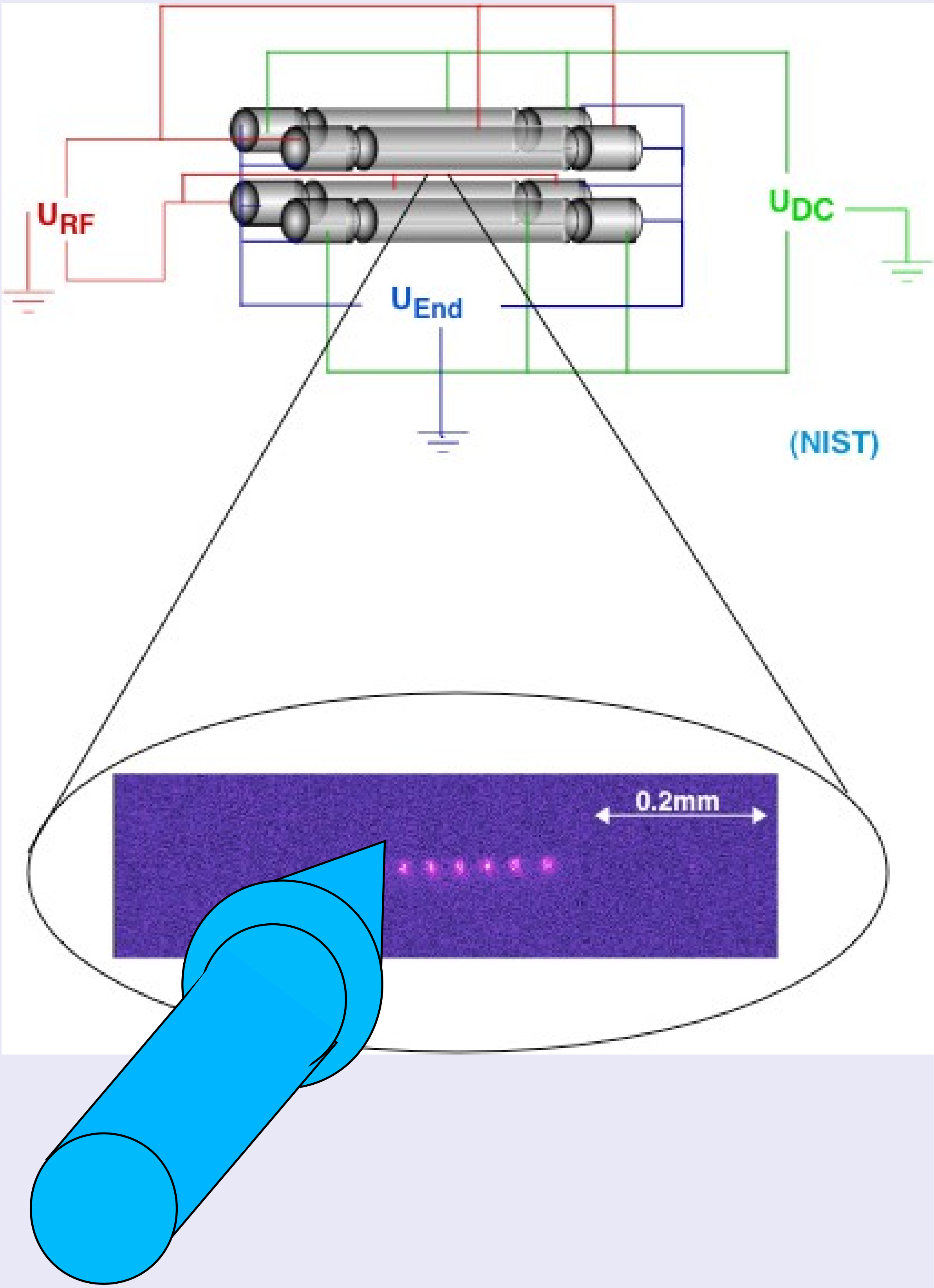
How do we build such a machine?

1. Quantum bits

2. Control: Focus lasers on ions.

- Read out information

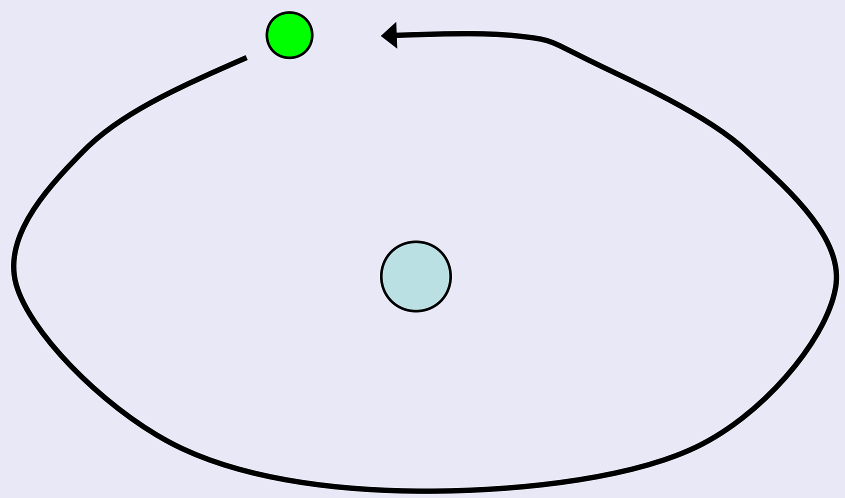
- Make atoms interact coherently



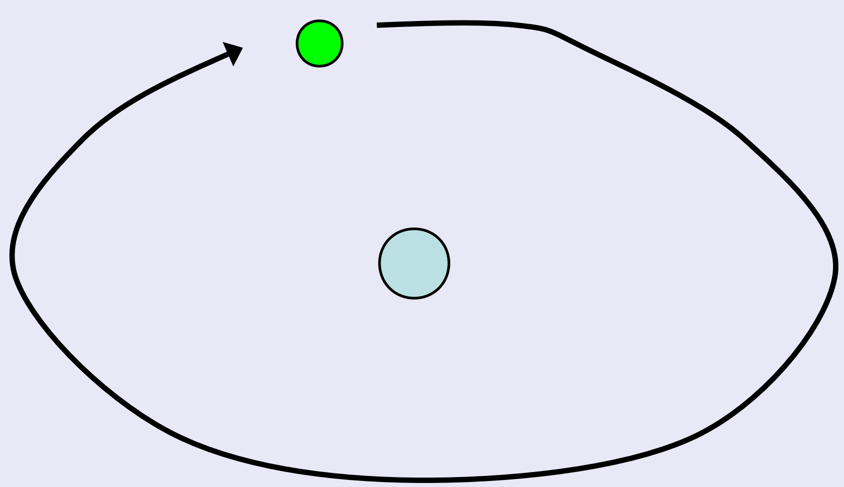
Quantum bits (Qubits)

A qubit is stored in an atom

”0”=



”1”=



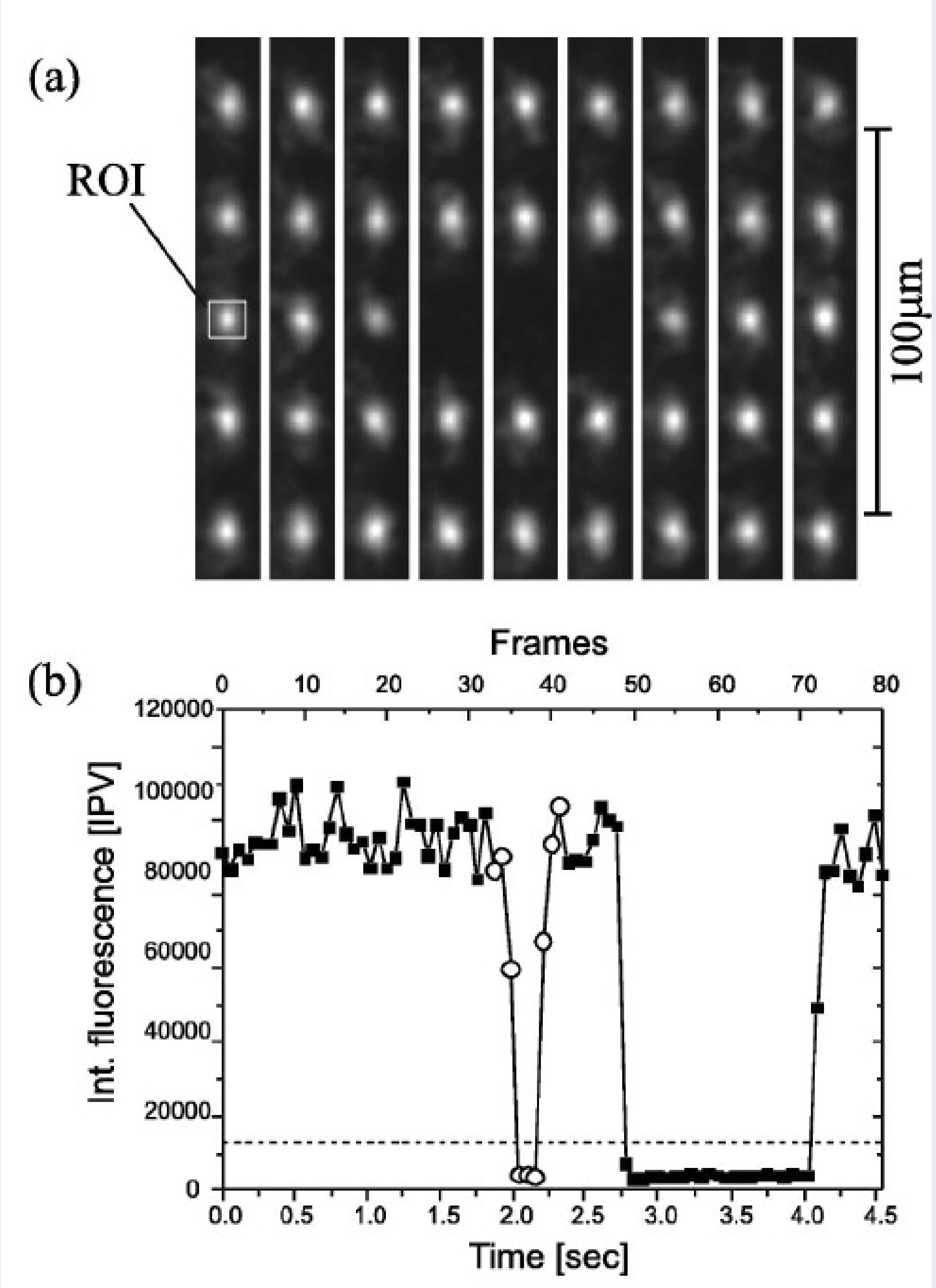
New: electrons can spin in either direction

Readout

Shine lasers on the ions.

Lights up if the atom spins in one direction.

No light if the atom spins in the other direction.

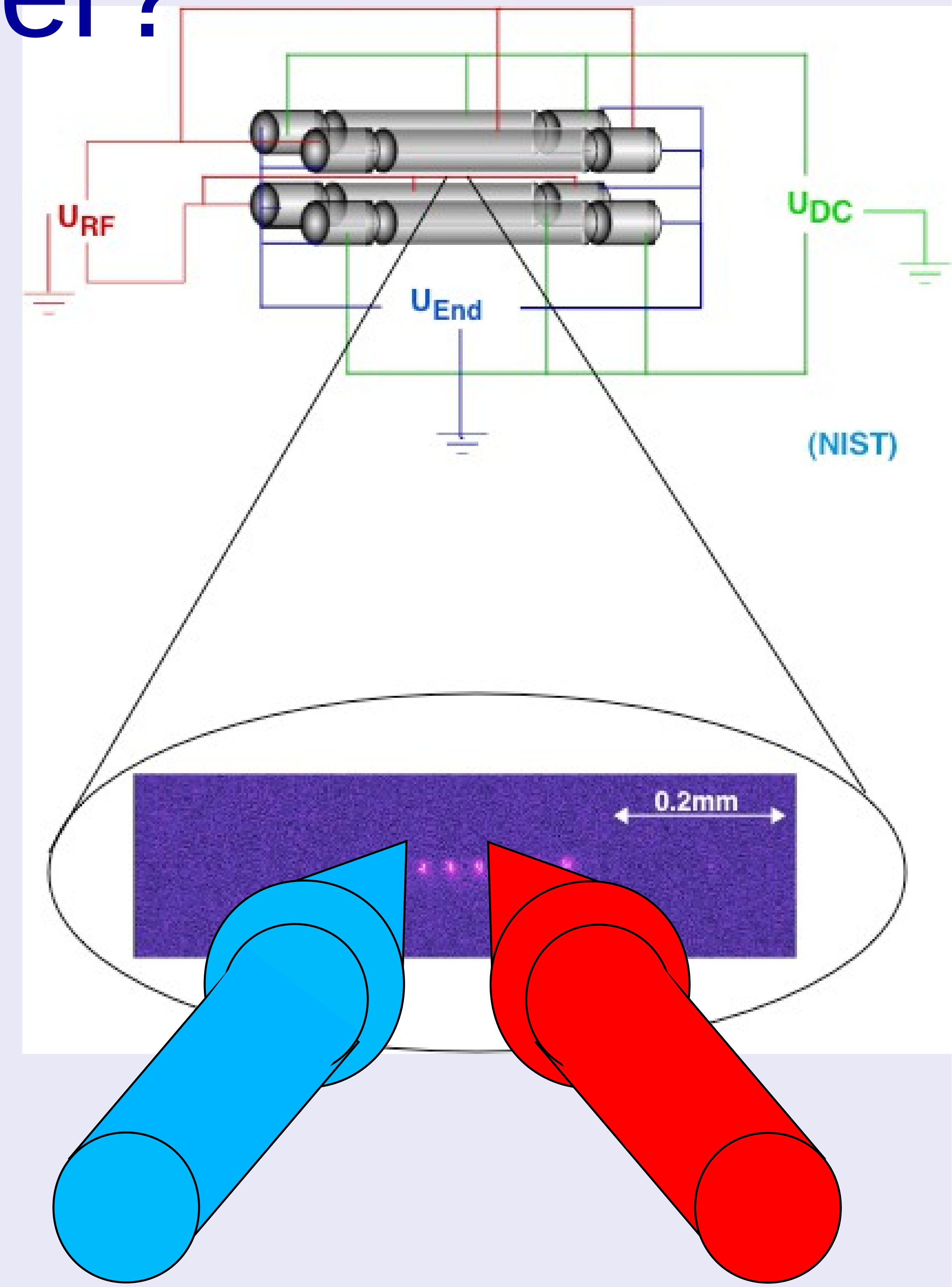


How do we build a quantum computer?

1. Quantum bits ✓
2. Control: focus lasers ✓

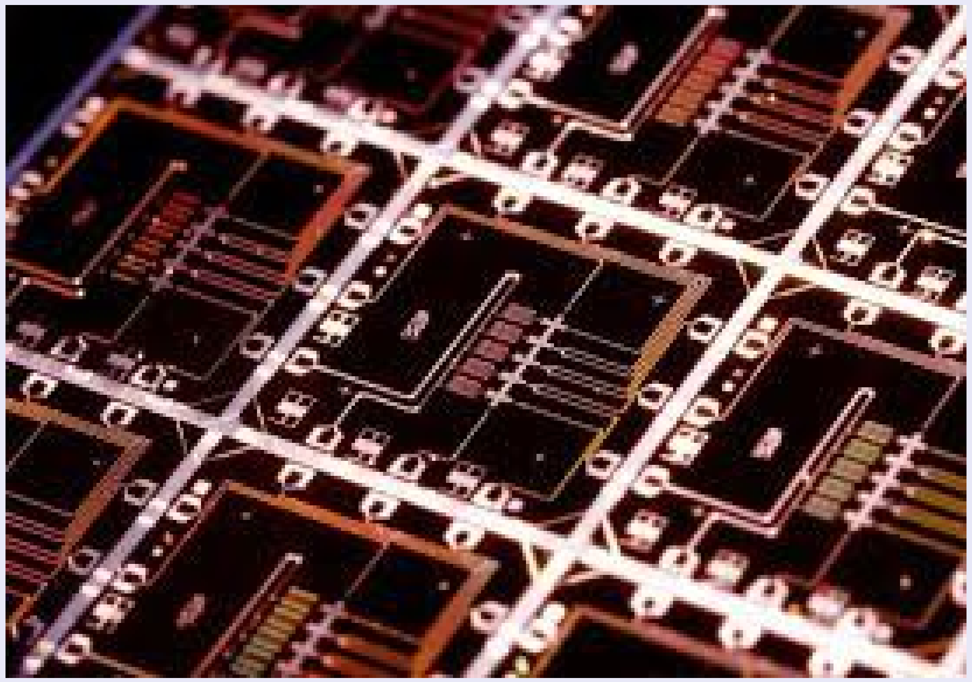
   on the ions ✓
3. Readout

   The hard part!
4. Make atoms interact

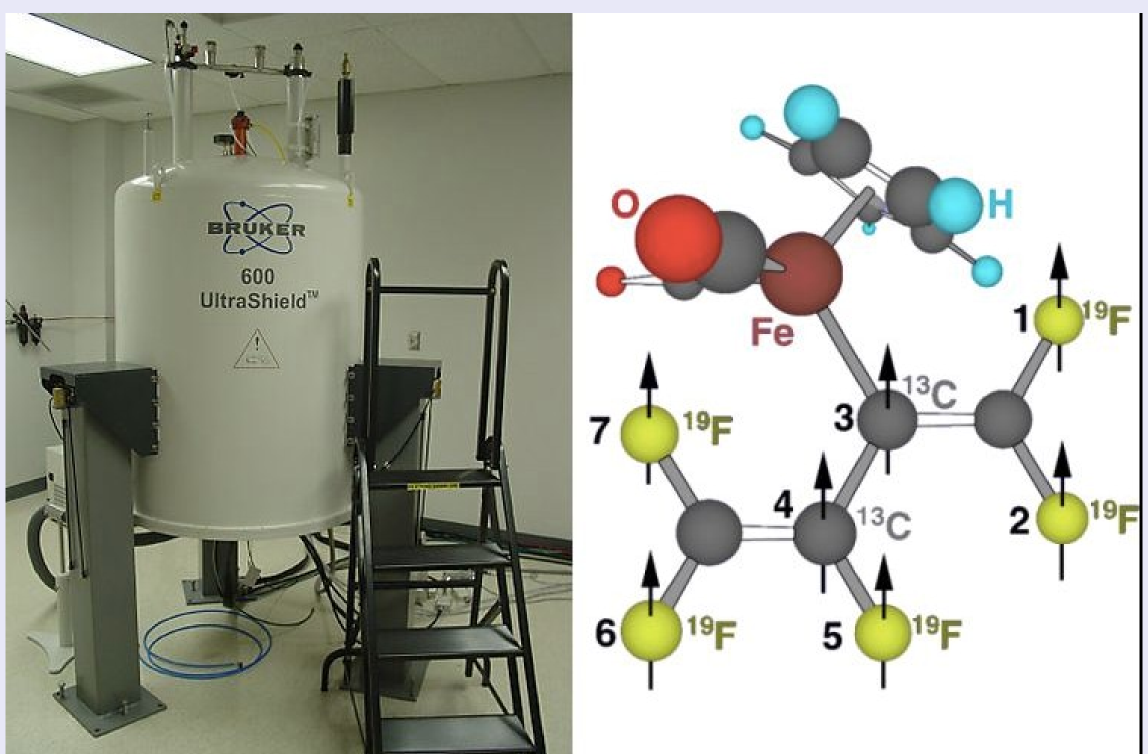


State of the art?

Controlled quantum systems

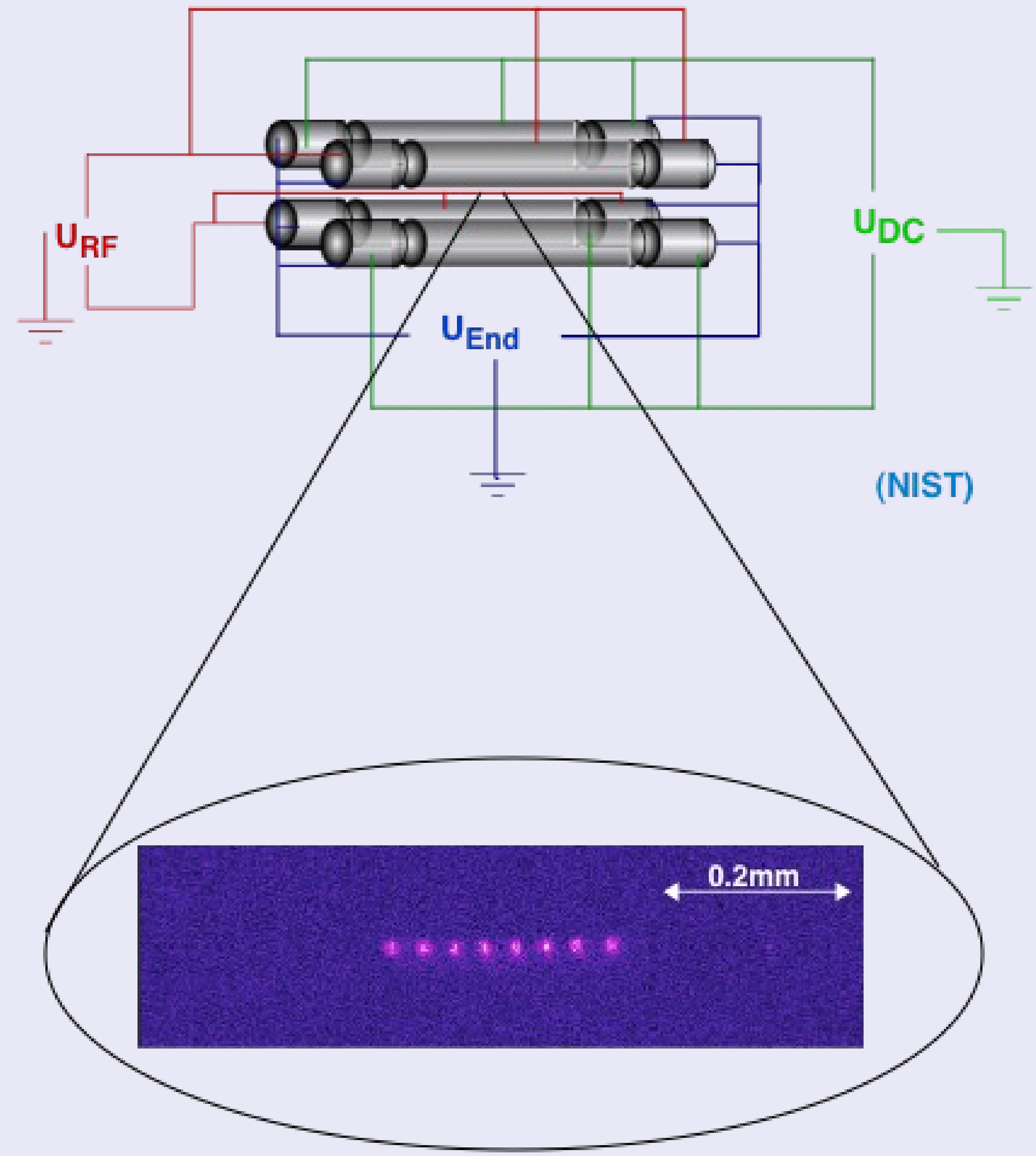


Superconducting circuit



NMR

Ions in a trap



No clear candidate for a quantum transistor

Quantum information Research

Industry

IBM, Microsoft, Google, Intel

Military

NSA, US Defence, Loockeed Martin

National Labs

NASA, NIST

Start-up companies

DWave, ID Quantique, Rigetti Computing

University Research

Over 100 groups around the world

2012 Nobel Prize in Physics

In Denmark:

QUANTOP, Qdev, Qmath, and many more.
Over 300 people involved in Quantum Info research

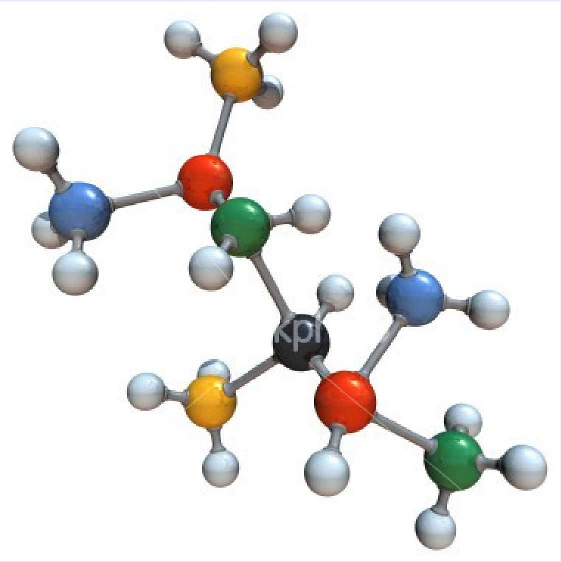
What will they be good for?

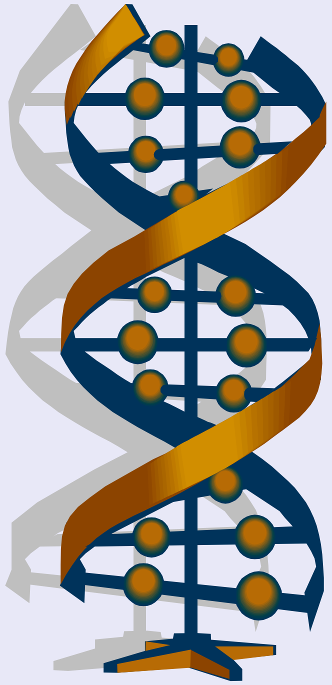
Metrology

Quantum information can lead to better measurement devices

Quantum simulations

Quantum computers can simulate other quantum systems





The future

10 years:
- Small quantum simulators
- Quantum metrology (gravitational detectors)

20 years:
- Small quantum processors
- Small quantum harddrives
- Quantum money?
- Practical quantum cryptography

40 years:
- Full blown quantum computer
- Unpredictable applications

All along the way: great insights into our physical laws.

Conclusion

Quantum mechanics is strange: objects can be at two different places at the same time

We can use this strangeness

- Quantum cryptography
- Quantum computing

IMPORTANT: its a lot of fun!

Quantum computers are soon a reality!

Thank you for your attention