Quantum Money, Teleportation and Computation

Steven Girvin

Yale University

ARDA

KECK FOUNDATION

LUX ET VERITAS

CRSNG NSERC

Quantum Uncertainty

Good news or bad?

We used to think it was bad, but now…

Haggar Physicists Develop 'Quantum Slacks'

DALLAS-At a press conference Monday, Haggar physicists announced the successful development of 'Quantum Slacks,' attractive, wrinkle-free pants that paradoxically behave like both formal and casual wear.

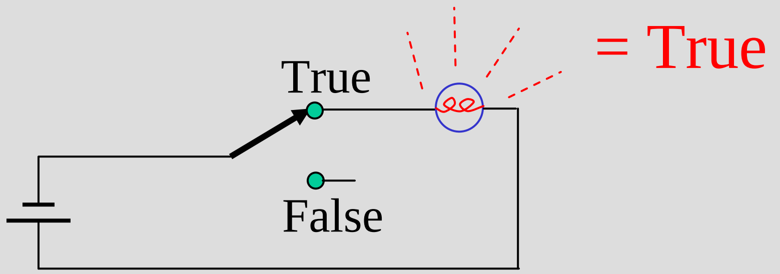
Classical bits

Answer to a ‘true-false’ or ‘yes-no’ question = 1 ‘bit’ of information

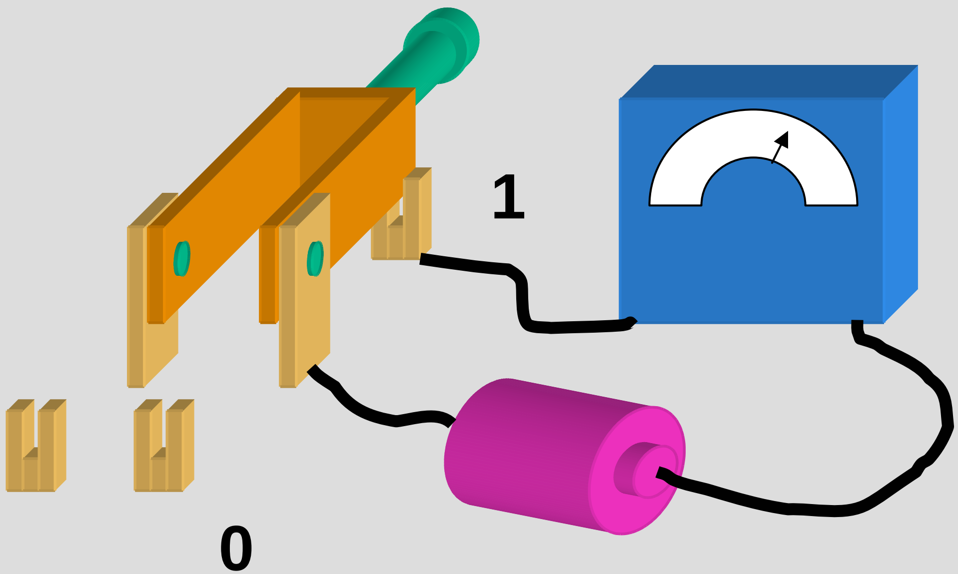
‘bit’=binary digit

Binary numbers: 10011= TFFTT

Am I tall?

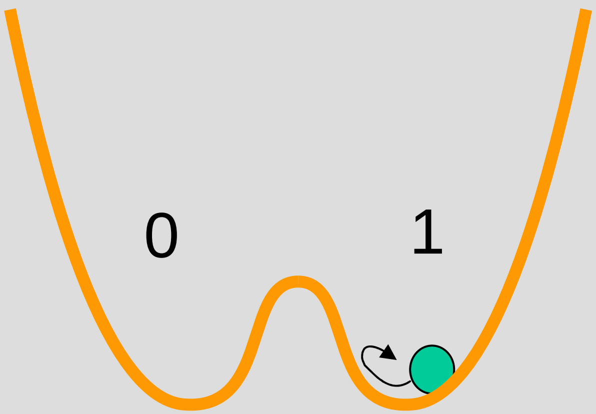


CLASSICAL INFORMATION



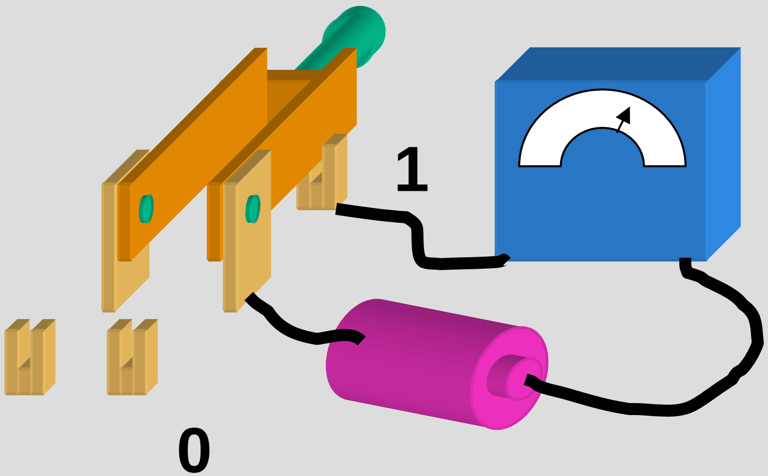
ONE BIT OF INFORMATION

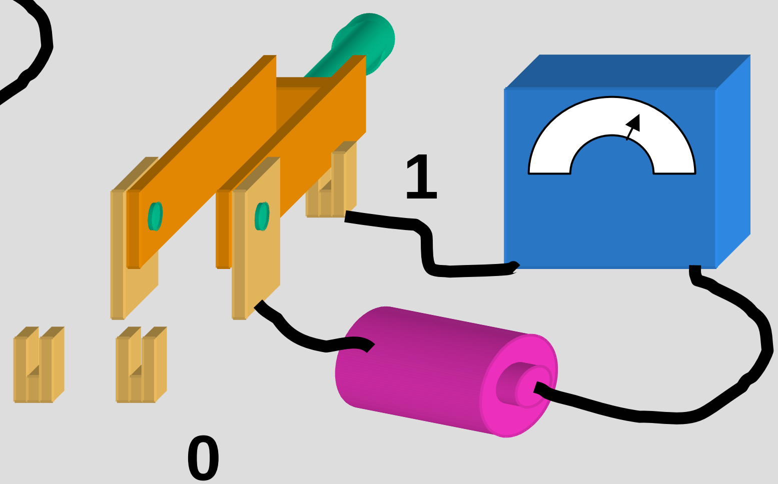
READOUT CAN BE MADE FAITHFUL



FAITHFUL READOUT

CLASSICAL INFORMATION CAN BE FAITHFULLY COPIED (‘CLONED’)

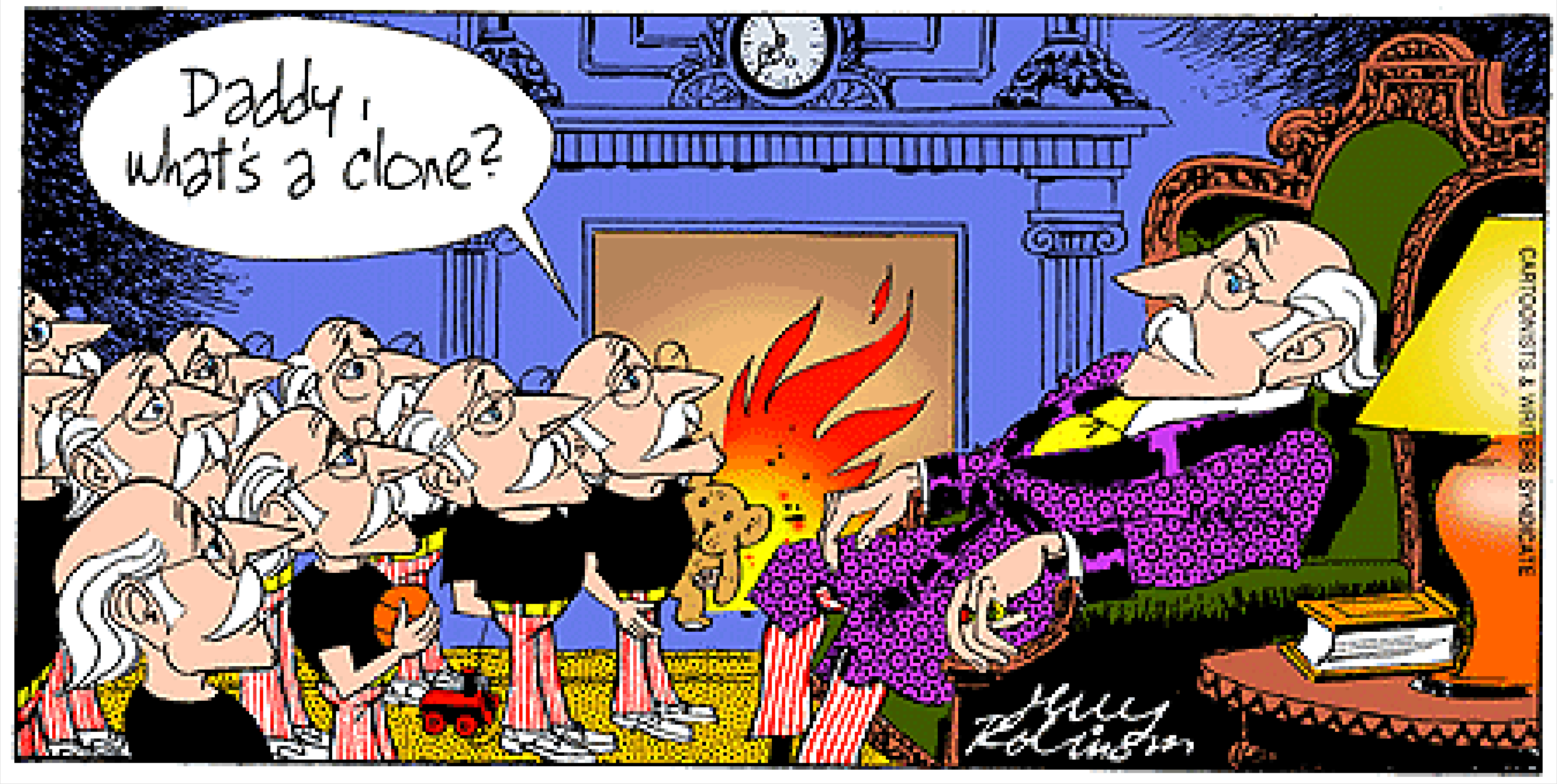




Recipe

- Measure 0 or 1
- Build a new 0 or 1

Cloning of Classical Systems is Possible



Quantum No Cloning Theorem

- Measurement affects the state of a quantum system
- More than one measurement is needed
- Resulting quantum uncertainty makes it impossible to make a perfect copy of a quantum system….

Quantum Teleportation

You *can* make a perfect copy of the quantum state of a system if you are willing to *destroy* the original.

Quantum Teleportation

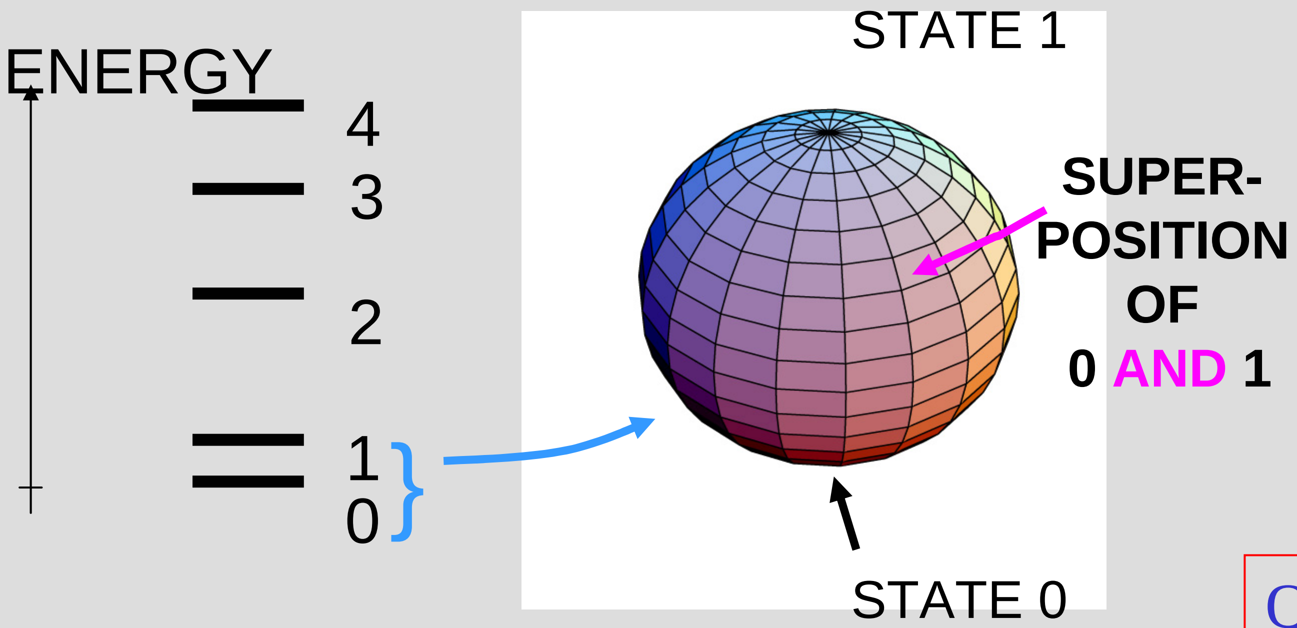
Original Destroyed

Perfect Copy Created

See: *Physics of Star Trek* by L. Krauss

Quantum Bits and Information

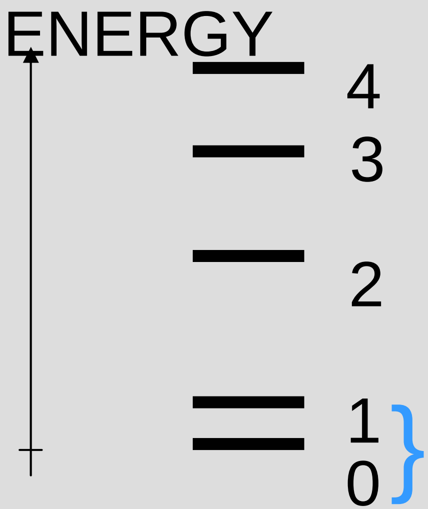
A quantum system with two distinct states 0,1 can exist in an infinite number of physical states *intermediate* between 0 and 1.

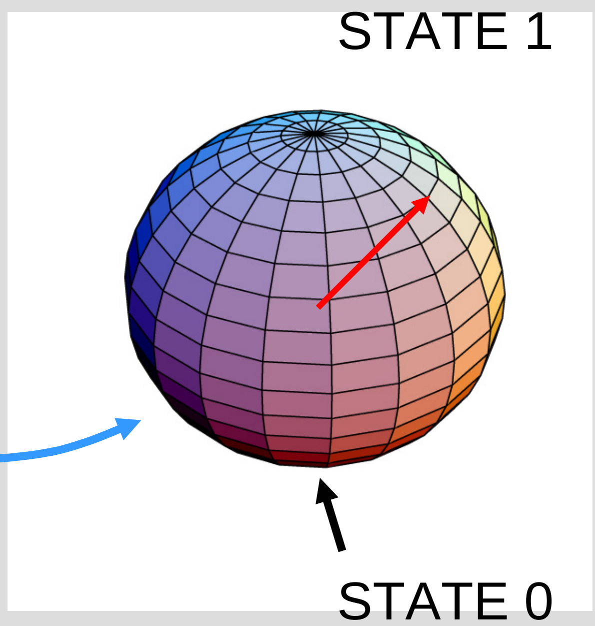


Quantum Bit = qubit

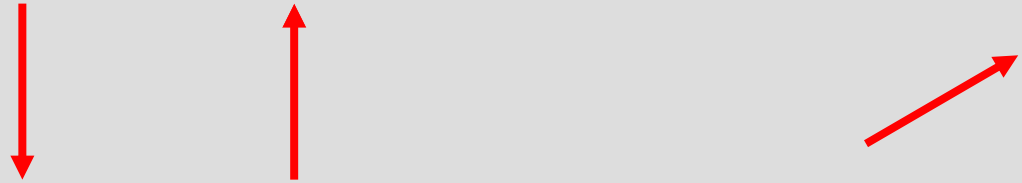
System can be in 'both states at once' (we are ***uncertain*** which state the qubit is in), just as it can take two ***paths*** at once.

Quantum Superpositions





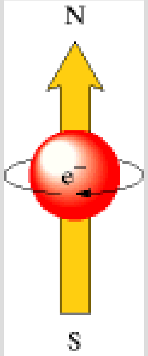
Each superposition state can be represented by an arrow (called the 'spin') pointing to a location on the sphere

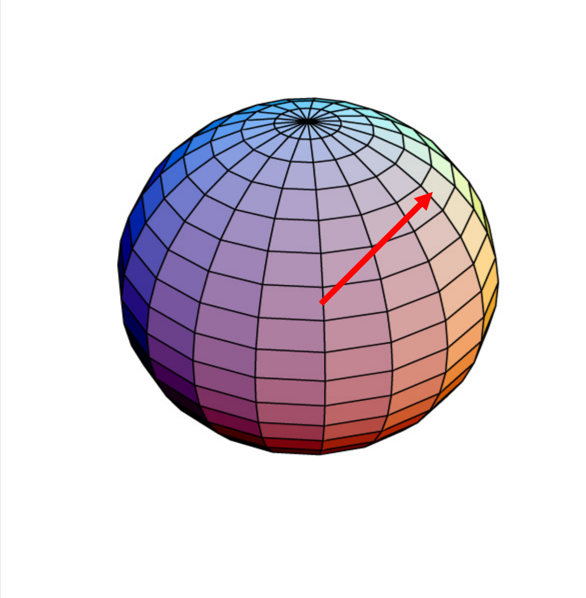


State 0 State 1 Intermediate state

Stern Gerlach Experiment

Silver atom has magnetic moment due to the electron 'spin'

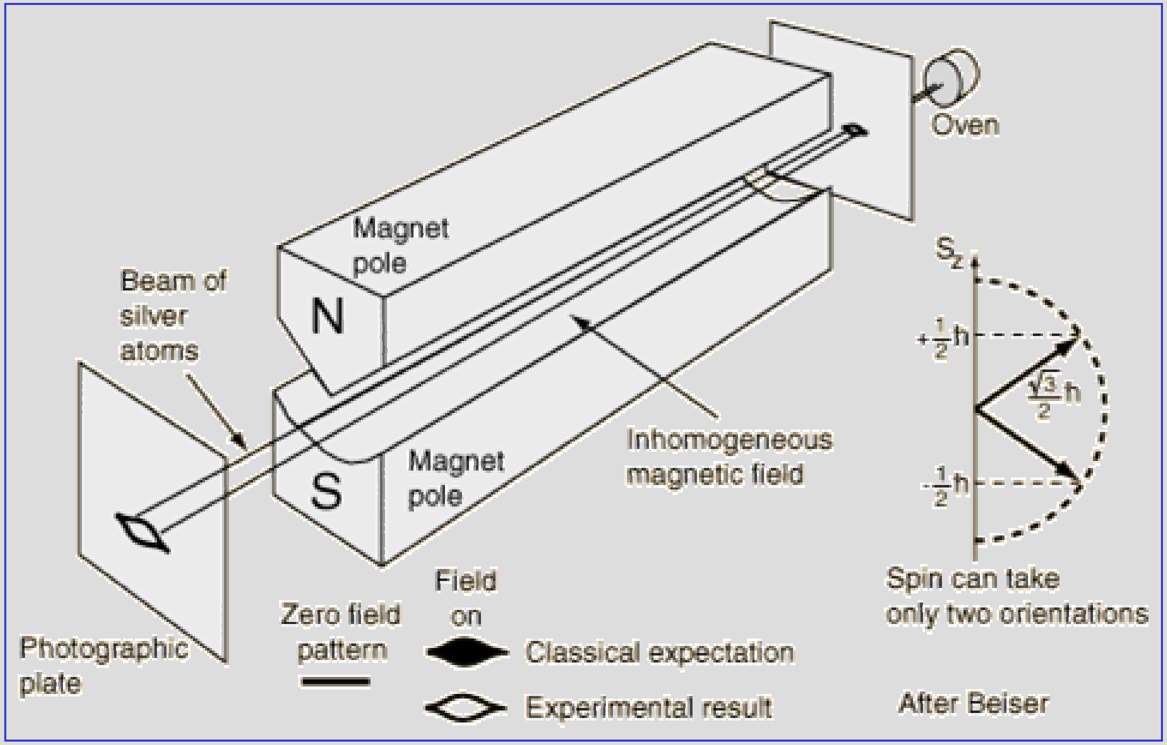




Magnetic moment (spin) can point in any direction and can be measured by passing the atom through a magnetic field gradient.

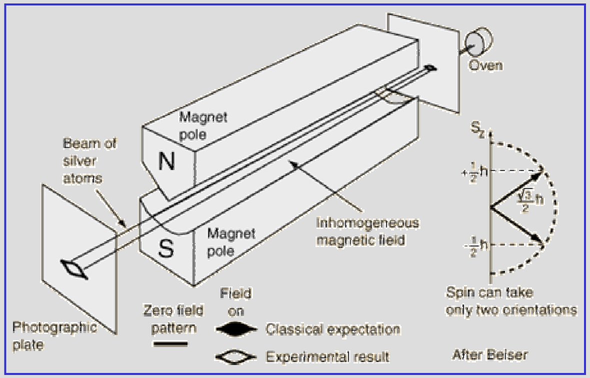
Stern Gerlach Experiment

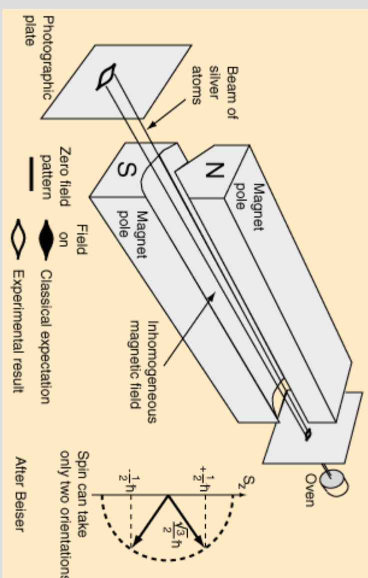
Silver atom has magnetic moment due to the electron ‘spin’



http://hyperphysics.phy-astr.gsu.edu

Bizzare Result #1





Electron spin always found to be perfectly aligned (or anti-aligned) with N-S axis:

N

Always this: ↑↓

S

N

Never this: ⇄

S

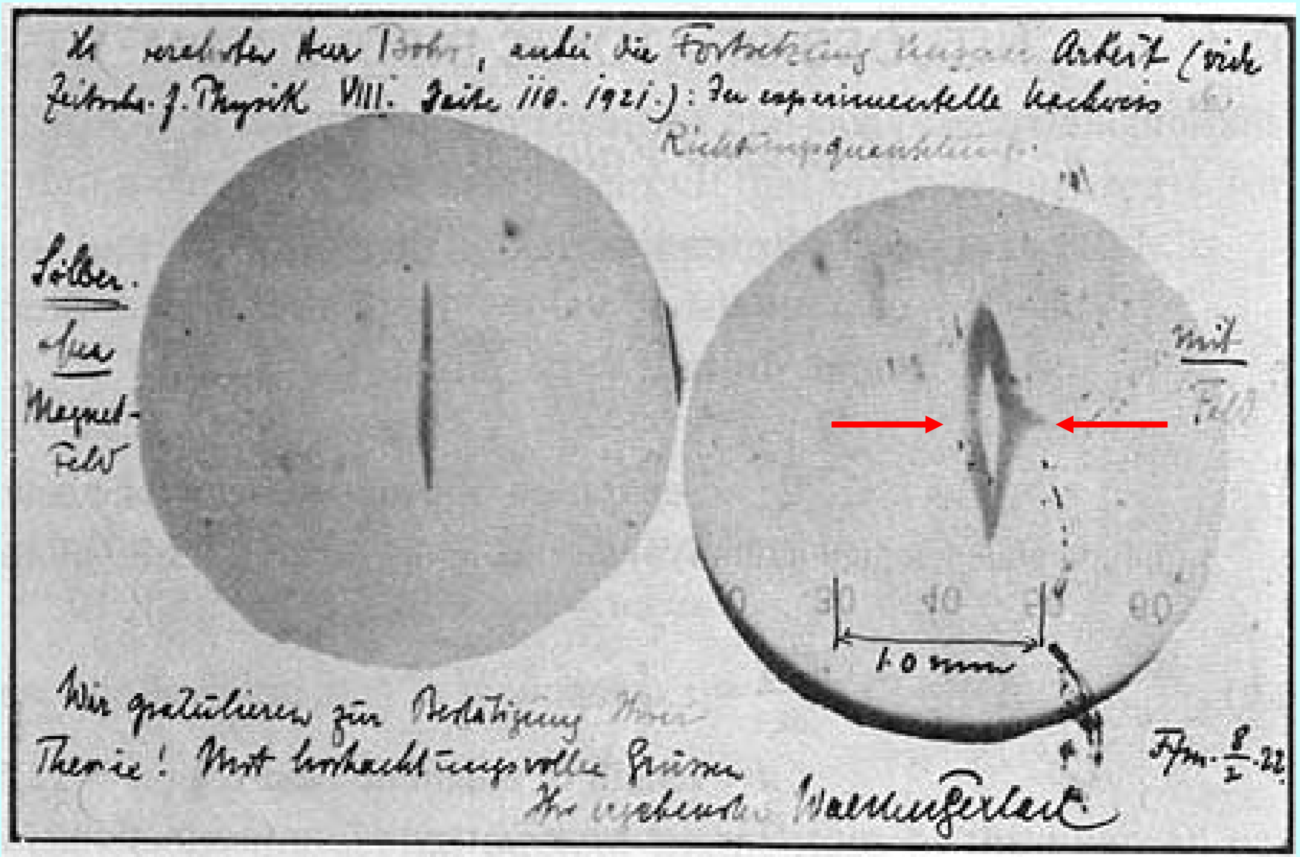
Always this:

S ⇄ N

Never this:

S ↑↓ N

Gerlach’s Postcard to Bohr



8 February 1922 ‘Attached [is] the experimental proof of directional quantization. We congratulate [you] on the confirmation of your theory.’

(Historical note: they did not realize this was the discovery of electron spin.)

AIP Emilio Segrè Visual Archives.

N

“Z measurement”

Always this: ↑↓ Never this: ⇄

S

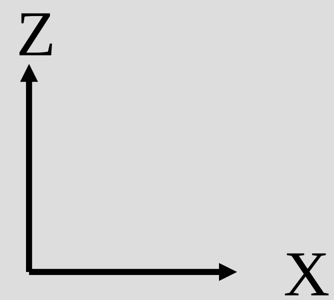
Always this: Never this:

“X measurement”

N ⇄ S N ↑↓ S

What is knowable?

Consider just 4 states:

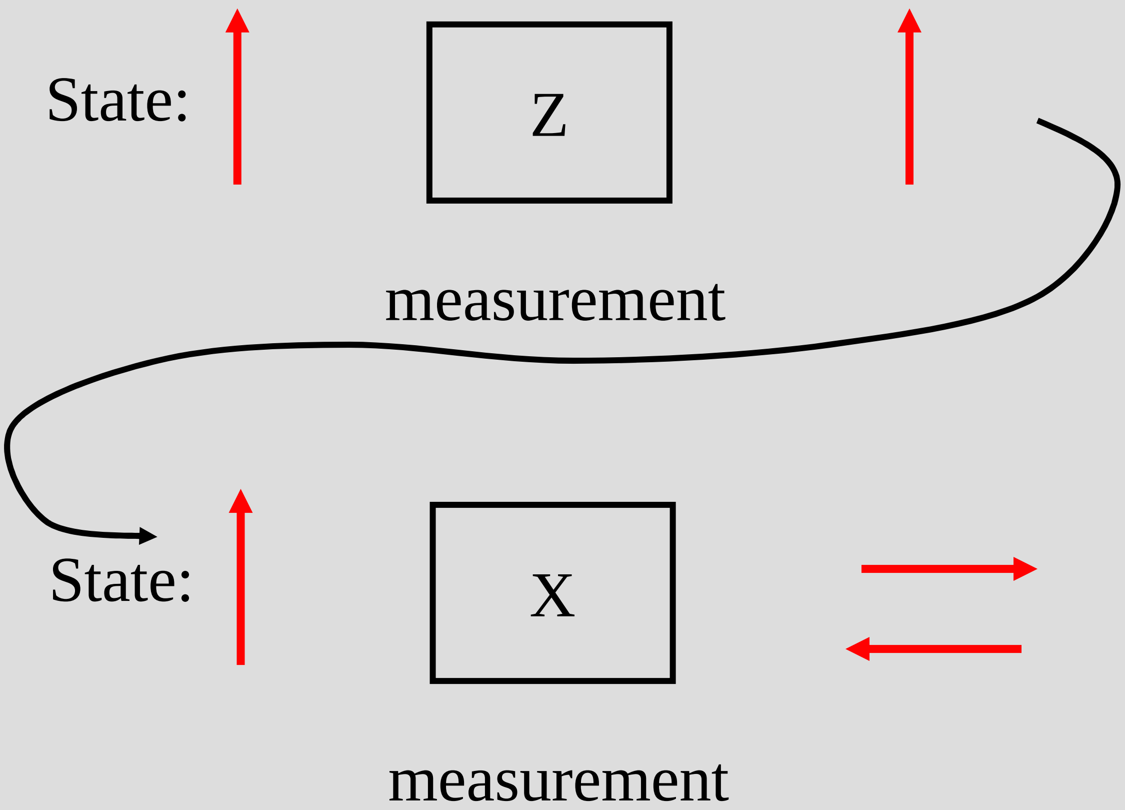


We are allowed to ask only one of two possible questions:

Does the spin lie along the Z axis? Answer is always yes! (± 1)
Does the spin lie along the X axis? Answer is always yes! (± 1)

BUT WE CANNOT ASK BOTH!
Z and X are ***INCOMPATIBLE*** OBSERVABLES

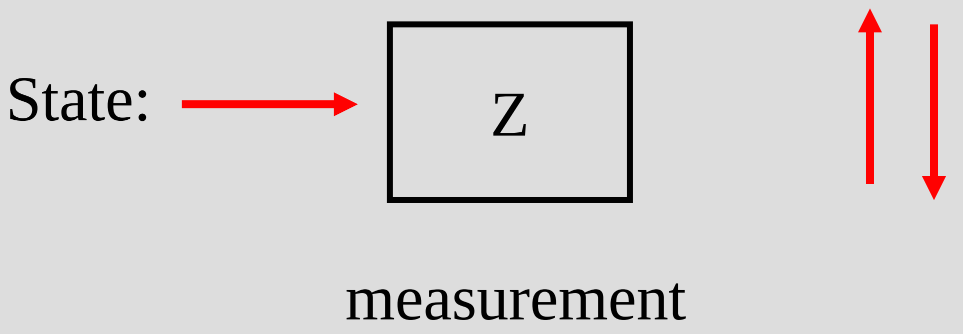
Measurements 1.



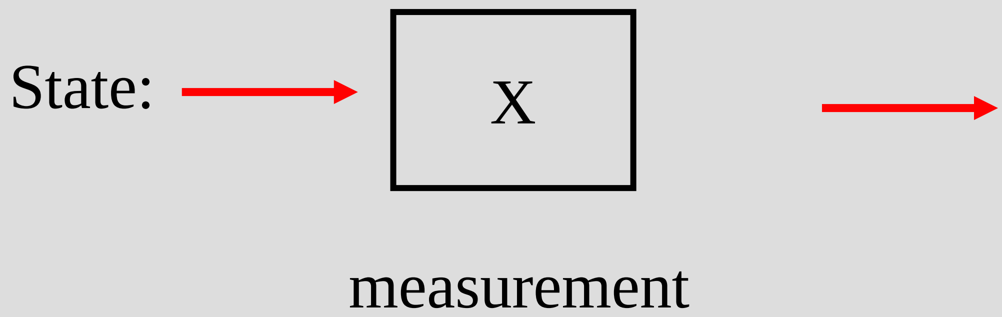
Result: +1 every time
State is unaffected.

Result: ±1 randomly!
State is *changed by measurement* to lie along X axis.

Measurements 2.

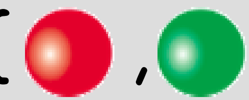


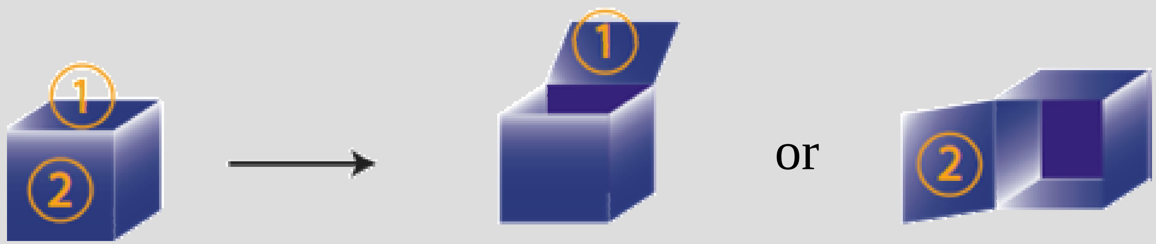
Result: ± 1 randomly!
State is *changed by measurement* to lie along Z axis.

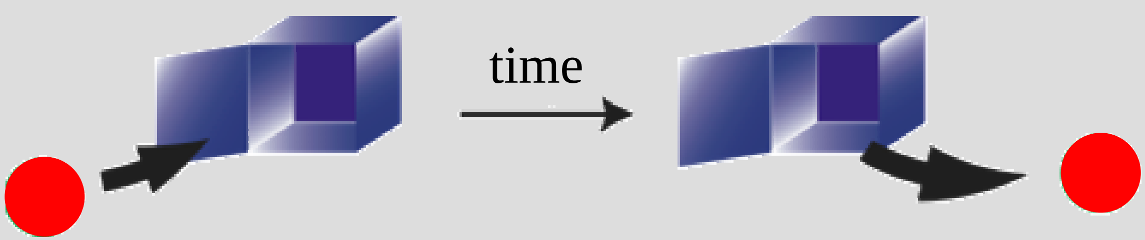


Result: +1 every time
State is unaffected.

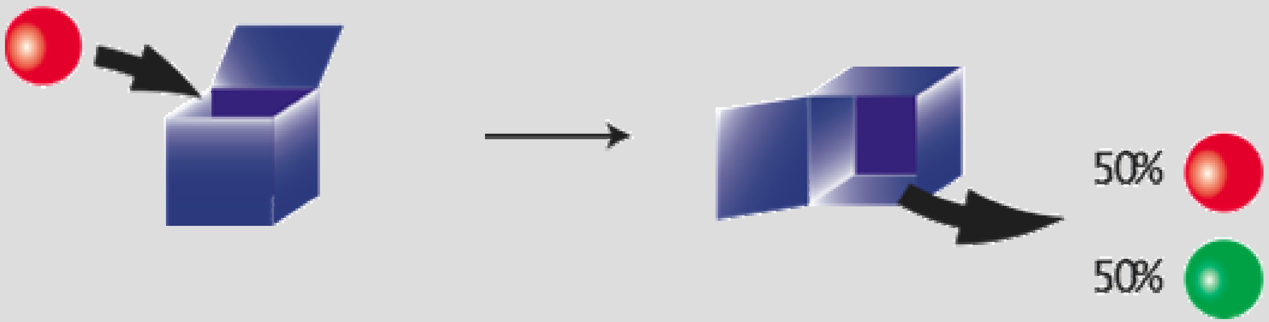
Fundamental Features of Quantum Information:

{0, 1} qubit ⟶ quball {  }





Quantum Strangeness



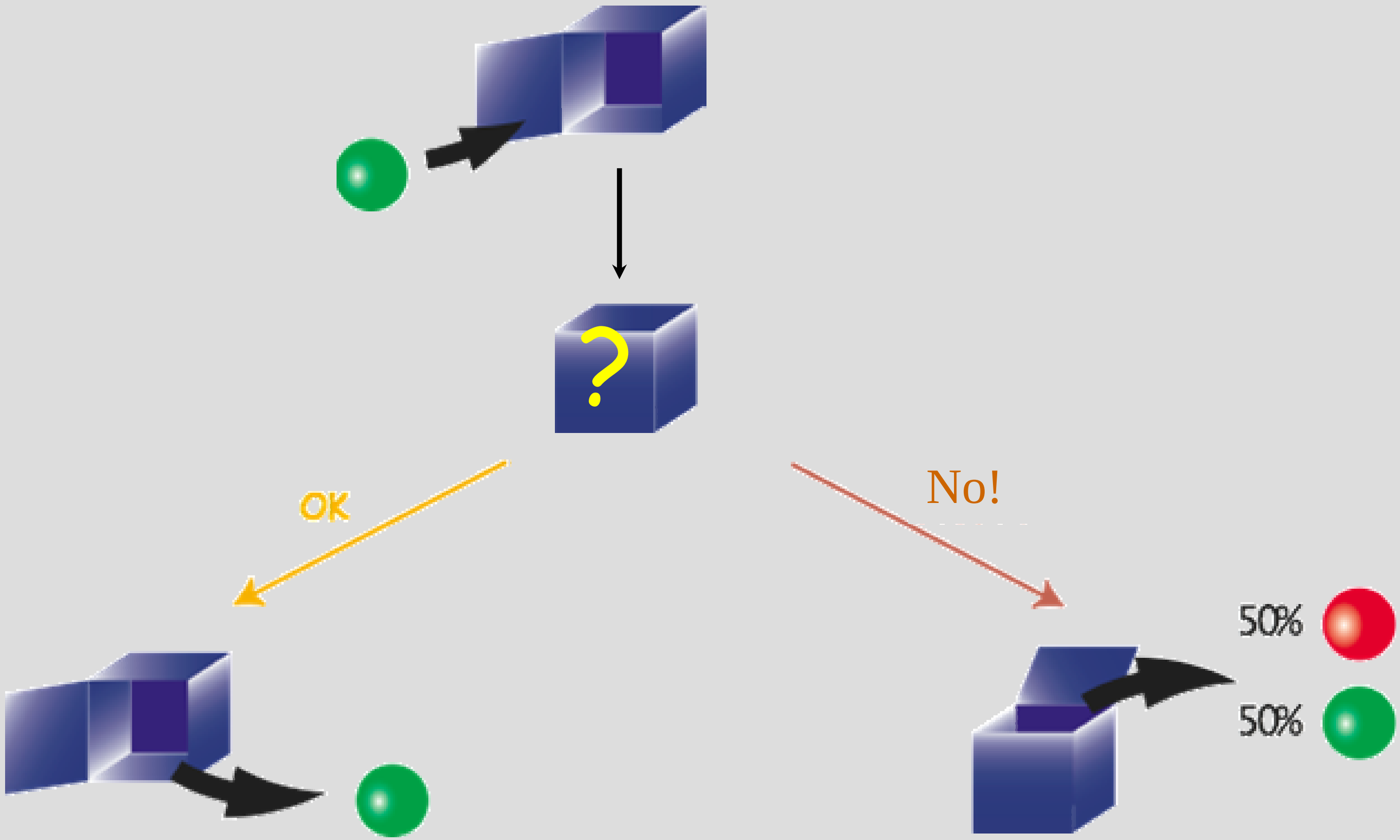
Result is random if prepared via one door and measured via another!

What is the state of the quball before measurement?

superposition of states : red + green

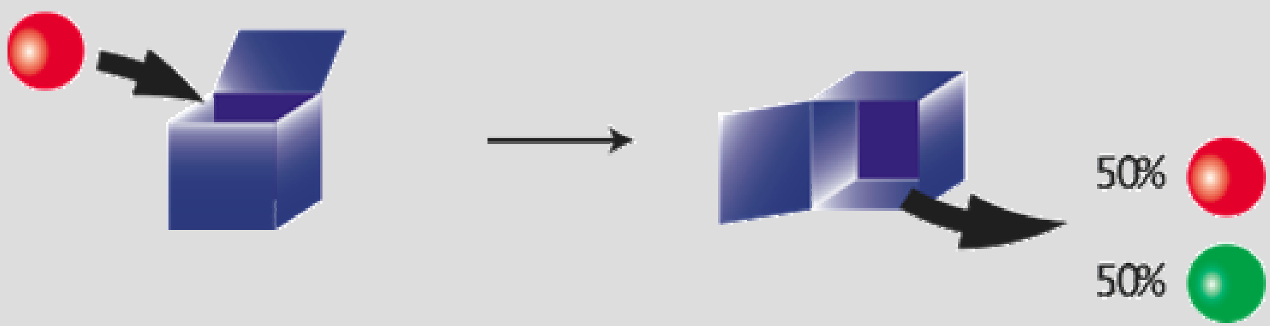
Measurement destroys the superposition.

Copying *unknown* state with certainty is impossible

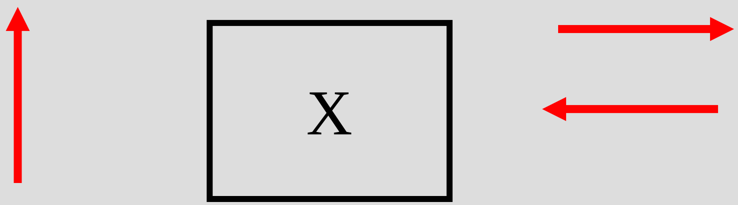


No Cloning Theorem

Given an unknown quantum state, it is ***impossible*** to make multiple copies



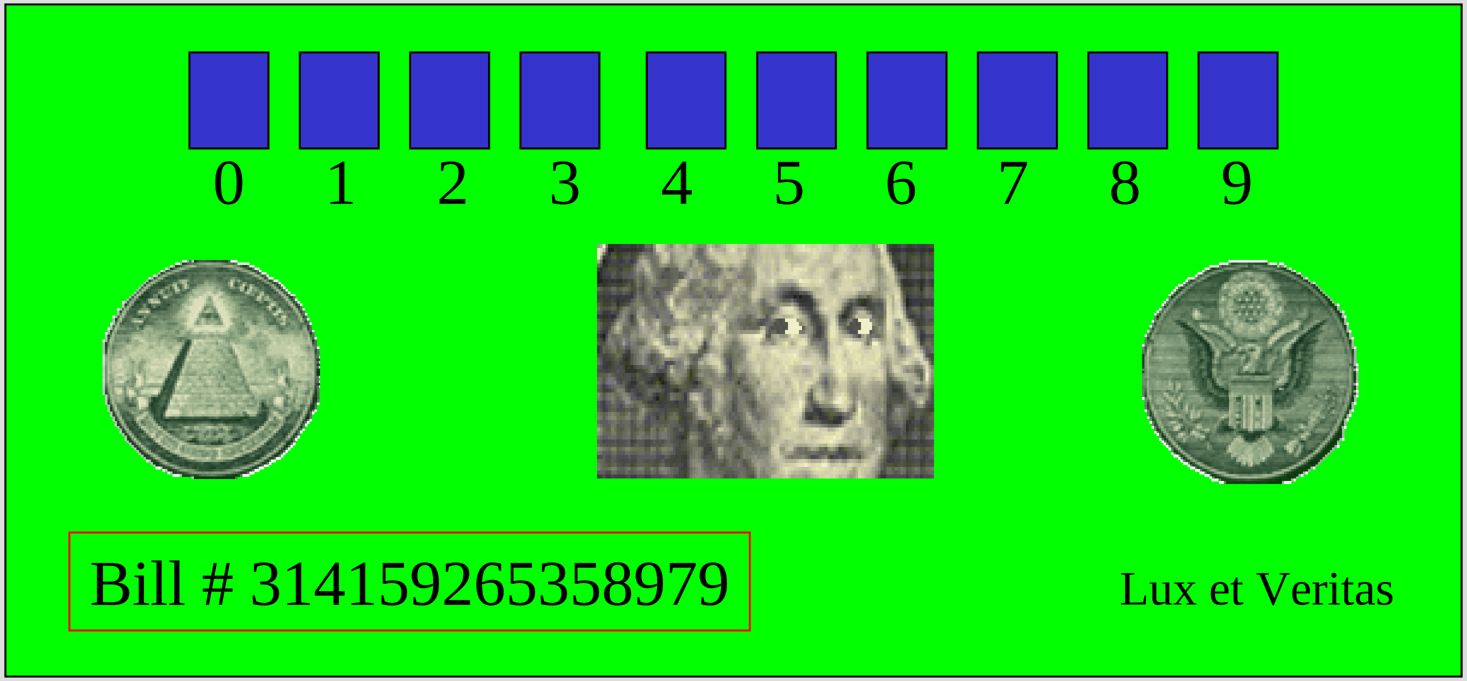
Unknown state:



Guess which measurement to make
("which door of box to open")
---if you guess wrong you change the state
and you have no way of knowing if you did….

Quantum Money

indeterminancy and incompatibility can be put to good use!



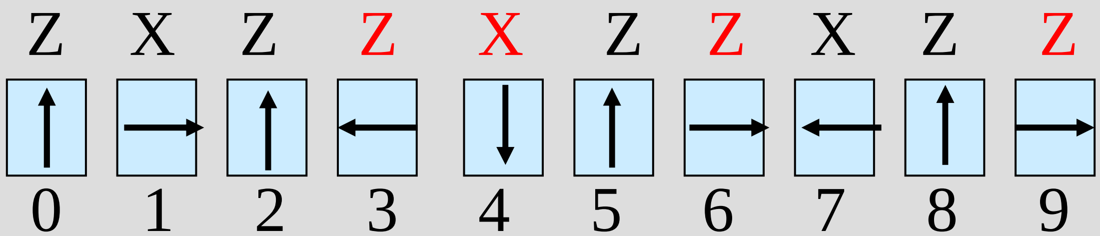
Each box contains a quantum system in 1 of 4 states:

↑, ↓, →, ←(*i.e.*, red or green inserted through door 1 or 2)

(S. Wiesner 1970)

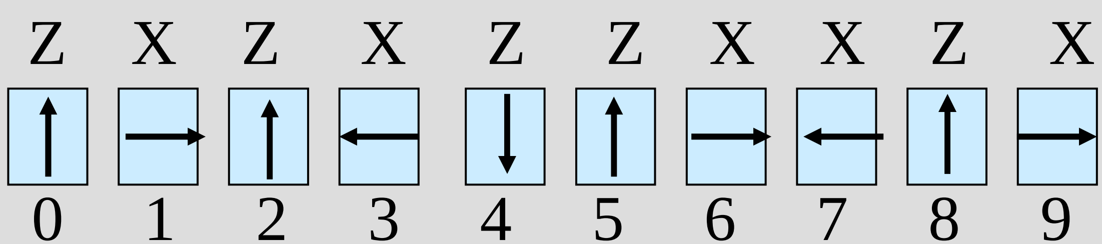
Is it Counterfeit?

Counterfeiter attempting to ‘clone’ the quantum state is forced to *guess* at orientations

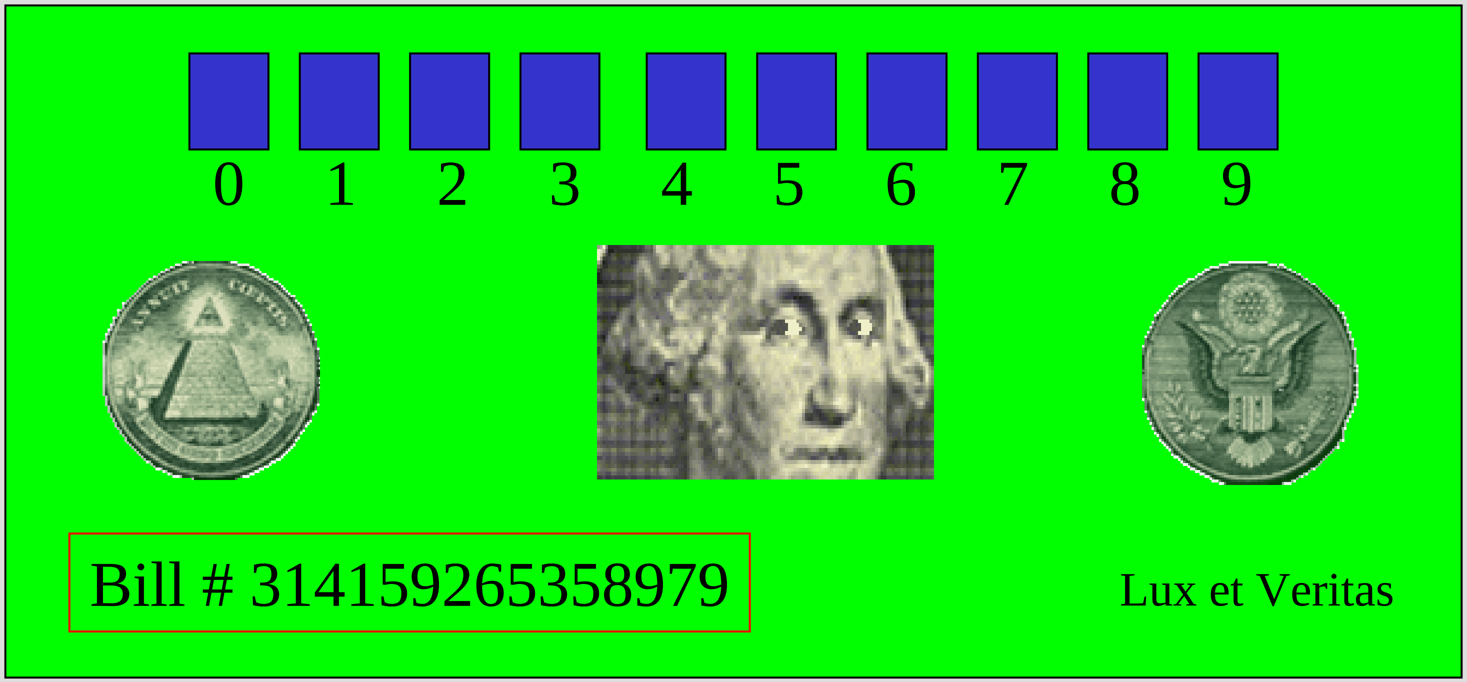


$$P_{\text{match}} = \left(3/4\right)^n = 0.056 \quad \text{for } n = 10.$$

Government issue detector orientations can be used to check validity (non-destructively)

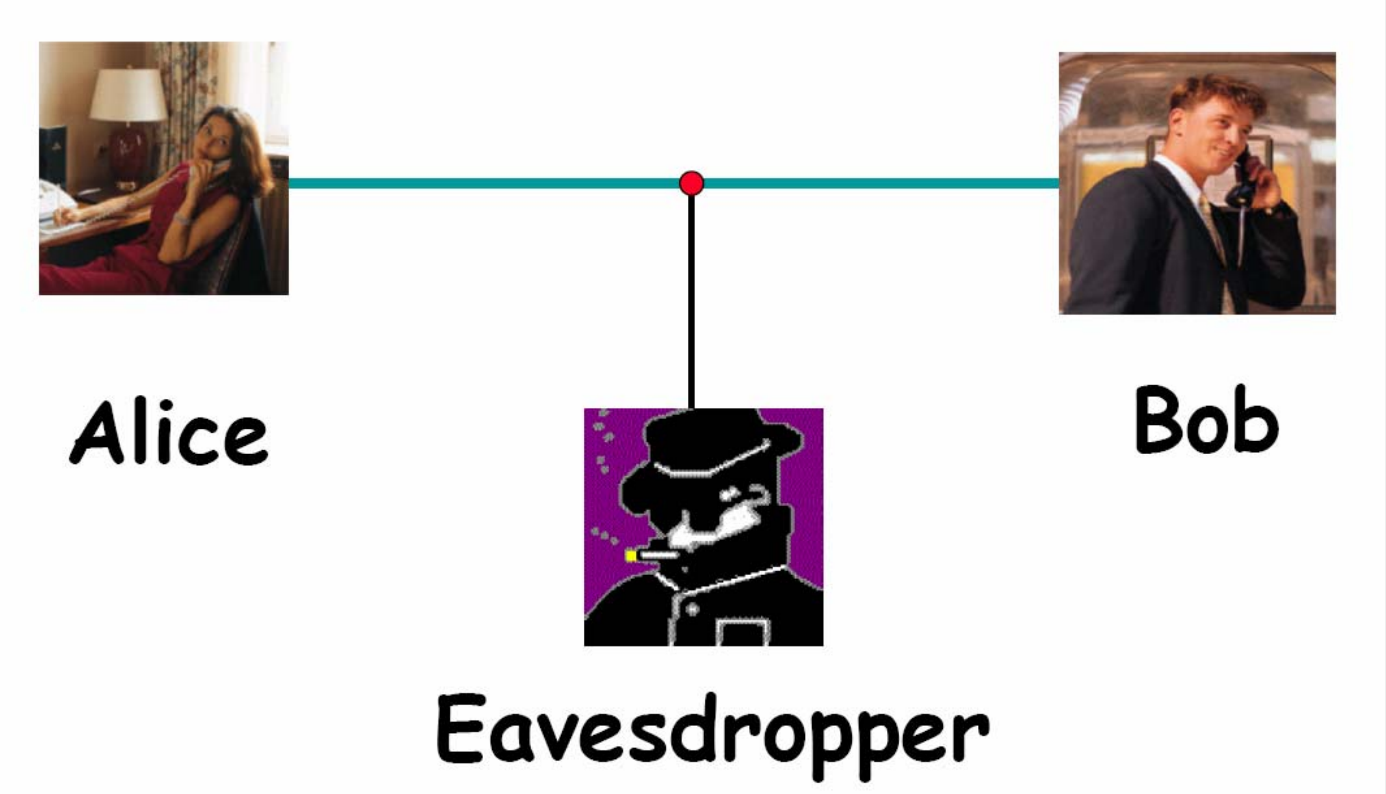


Quantum Money



Don't leave home without it!

Quantum Cryptography



(After Artur Ekert)

One-time pad

plaintext	0	1	0	0	1	0	1	1	0	1
key	0	1	1	1	1	0	1	0	1	0
cryptogram	0	0	1	1	0	0	0	1	1	1

Perfectly secure if the key is:

- **RANDOM**
- **AS LONG AS THE MESSAGE**
- **NEVER REUSED**

Addition mod 2: 0+0=0, 0+1=1, 1+0=1, 1+1=0

(After Artur Ekert)

Key distribution problem

?

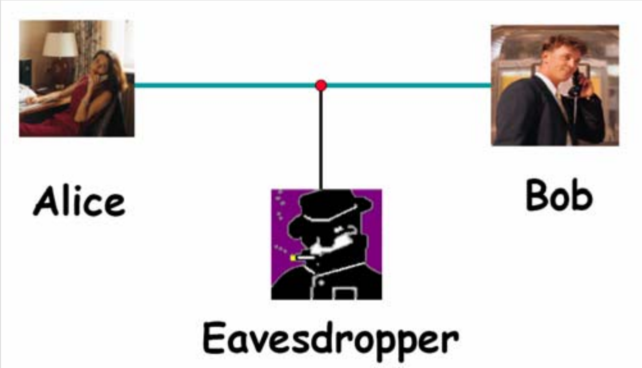
KEY	0	0	1	0	1	1	0

KEY	0	0	1	0	1	1	0

Solution: Distribute Key as Quantum Money

(After Artur Ekert)

Quantum Key Distribution



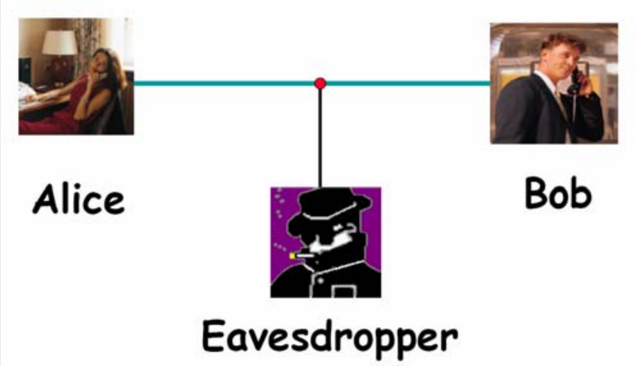
Alice sends Bob some quantum money

Z	X	Z	X	Z	Z	X	X	Z	X
↑	→	↑	←	↓	↑	→	←	↑	→
0	1	2	3	4	5	6	7	8	9

Bob chooses random detector orientations but gets half of them wrong

Z	X	Z	Z	X	Z	Z	X	Z	Z
↑	→	↑	←	↓	↑	→	←	↑	→
0	1	2	3	4	5	6	7	8	9

Quantum Key Distribution



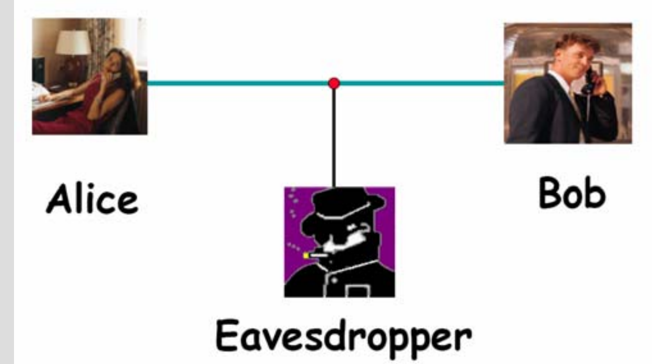
Alice announces the correct detector orientations

Z	X	Z	X	Z	Z	X	X	Z	X
↑	→	↑	←	↓	↑	→	←	↑	→
0	1	2	3	4	5	6	7	8	9

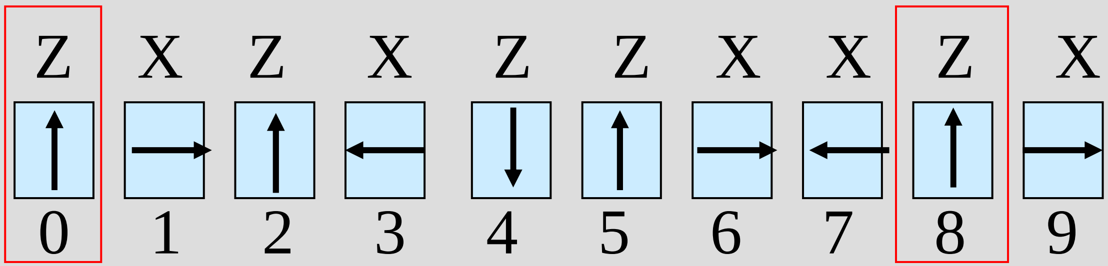
Bob discards the ones he got wrong

Z	X	Z	~~Z~~	~~X~~	Z	~~Z~~	X	Z	~~Z~~
↑	→	↑	~~←~~	~~↓~~	↑	~~→~~	←	↑	~~→~~
0	1	2	~~3~~	~~4~~	5	~~6~~	7	8	~~9~~

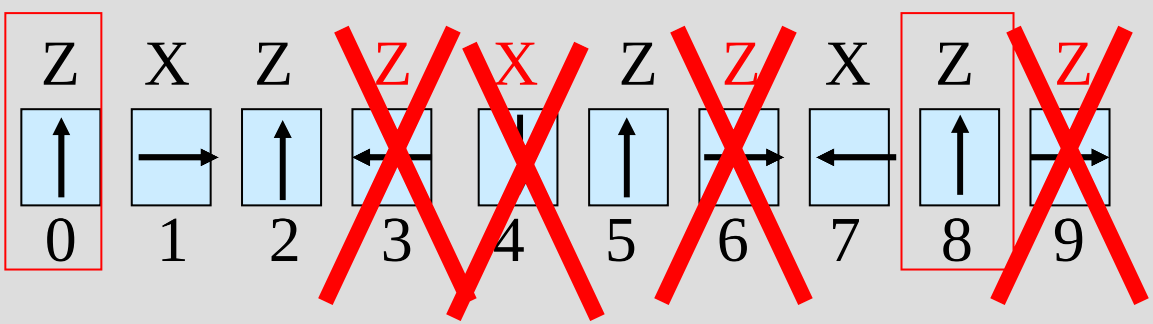
Quantum Key Distribution



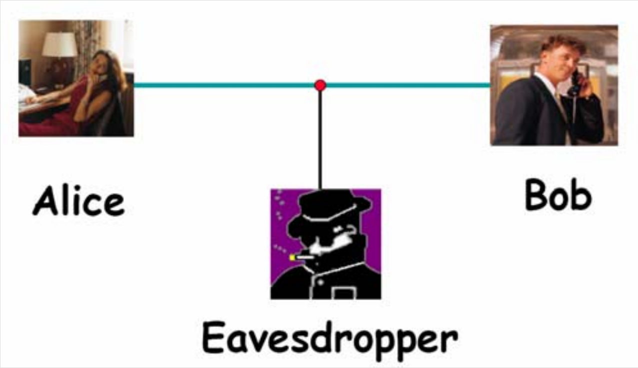
Alice announces the contents of a random subset of the boxes



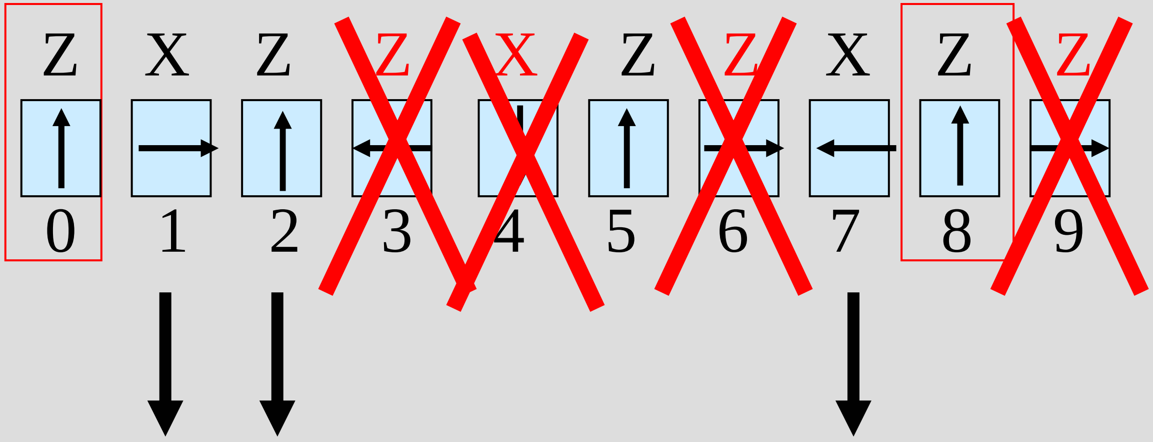
Bob checks to see if he got the same result. If yes, then no eavesdropper has corrupted the data by opening the boxes and then cloning.



Quantum Key Distribution

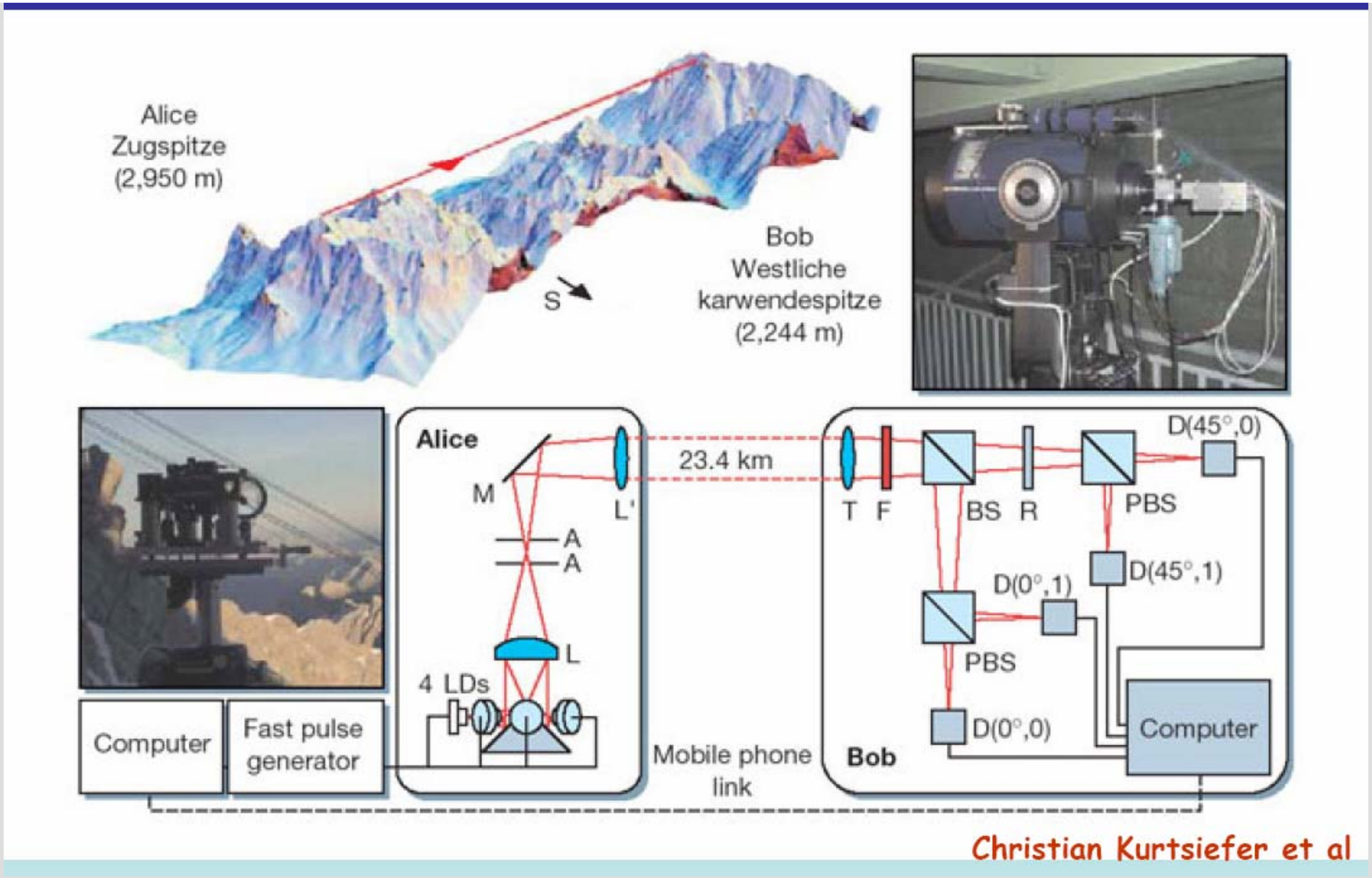


Bob and Alice use the remaining orientations as the key because their measurements are guaranteed to agree.



The key: 1 1 0 ….

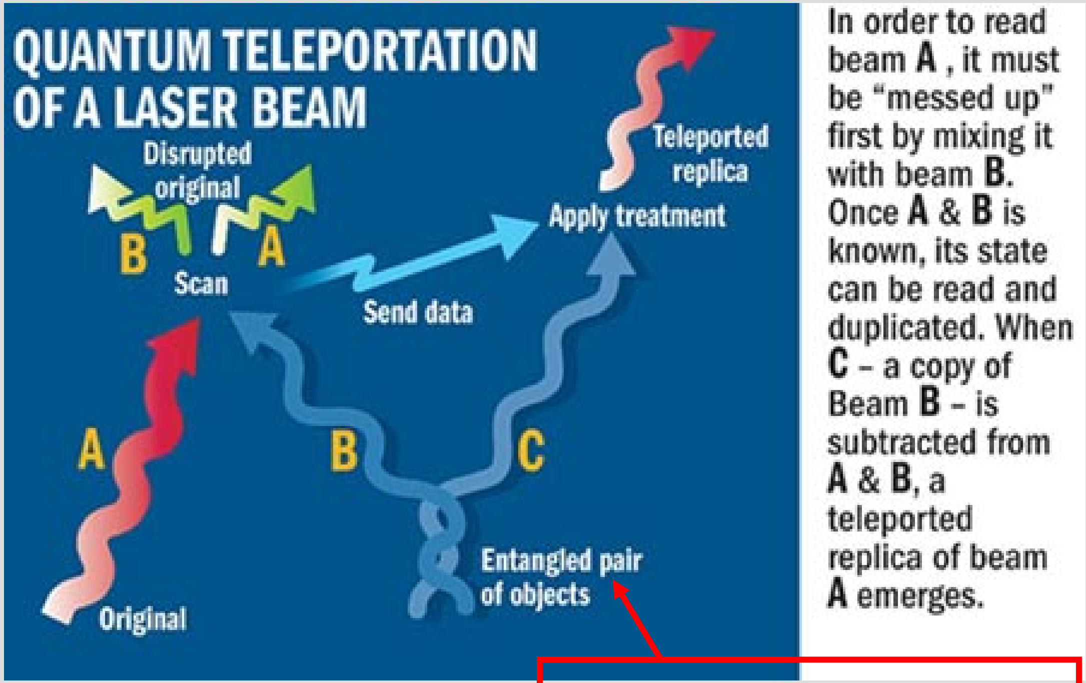
Quantum Key Distribution via photon beams through air or optical fibers



Quantum Teleportation

You *can* make a perfect copy of the quantum state of a system if you are willing to *destroy* the state of the original (required by no cloning theorem.)

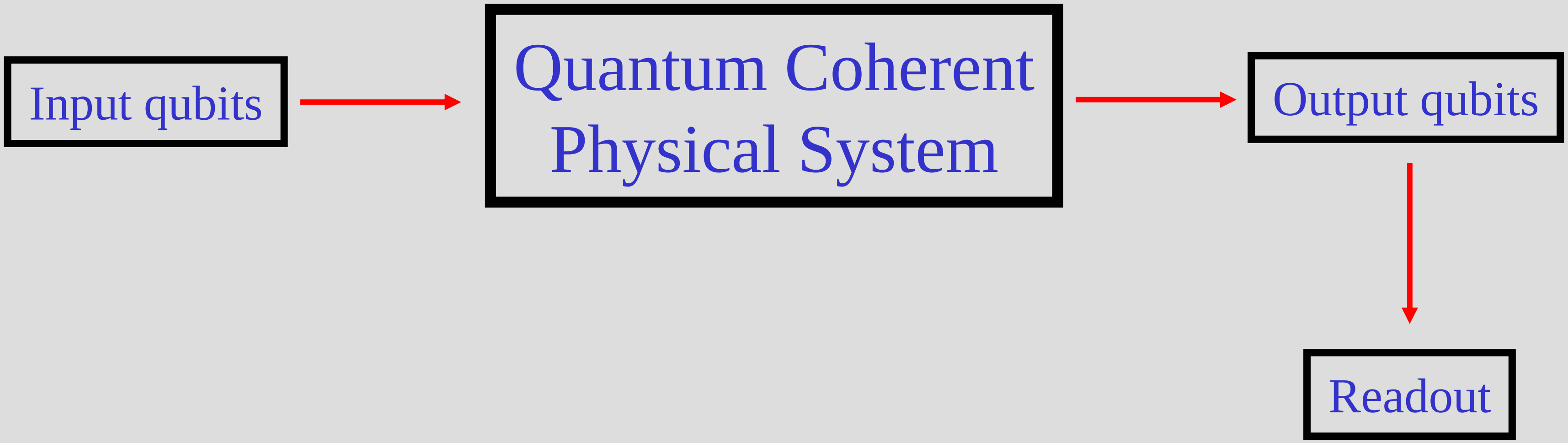
EPR: 'spooky action at a distance'



New quantum resource

It is important not to make errors during teleportation

Quantum Computation



Quantum Parallelism:
Input can be in many states at once!

Danger: so is the output!

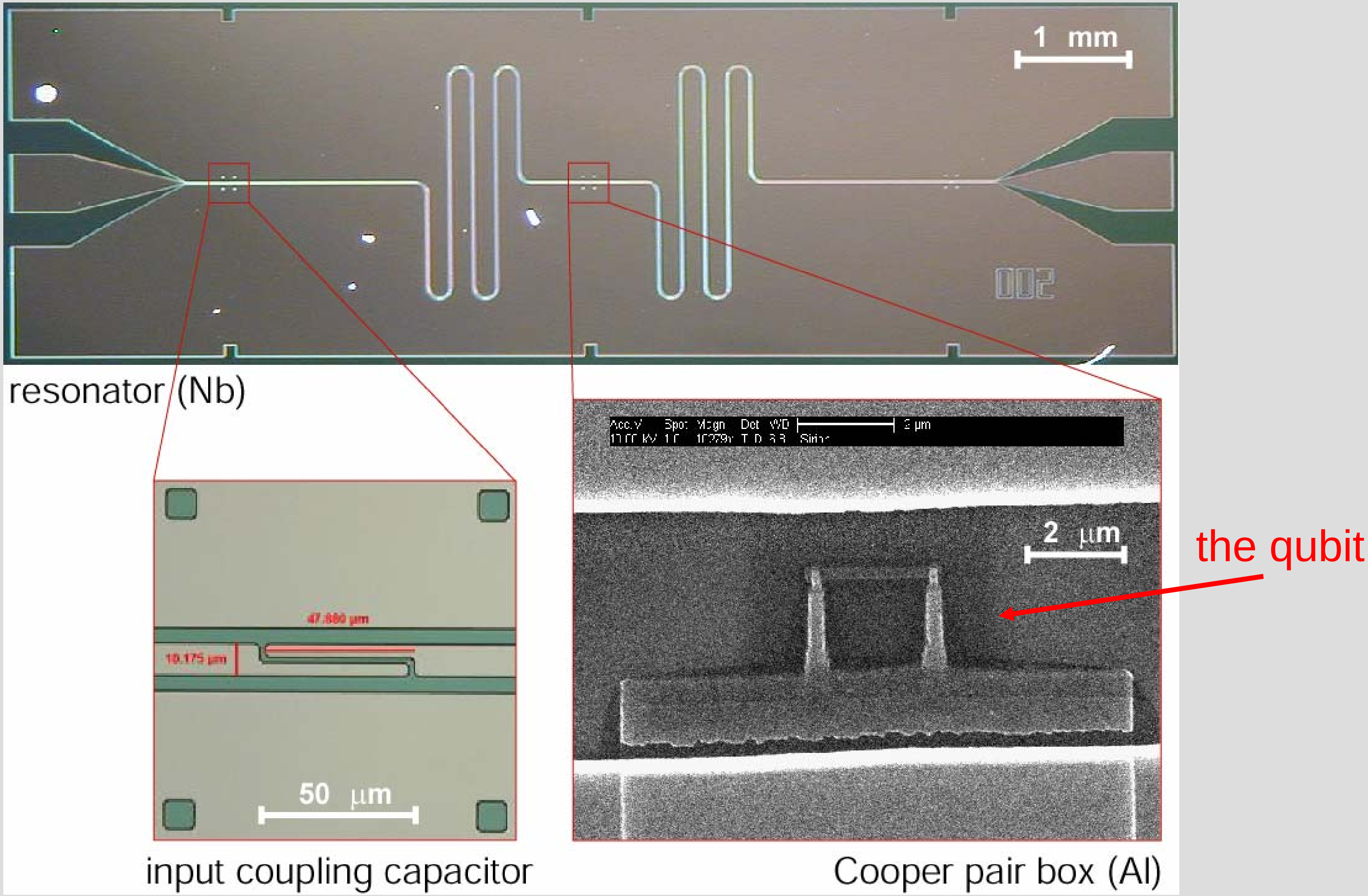
(Few) known algorithms:
-factoring
-searching

Physical Realizations of Qubits

- trapped ions (Boulder, Ann Arbor,…)
- liquid phase NMR
- quantum dots (electrons or excitons)
- electrons on liquid helium
- …….
- Superconducting Josephson junctions
- Superconducting Cooper pair boxes

Field is still in its infancy: 1-4 bits

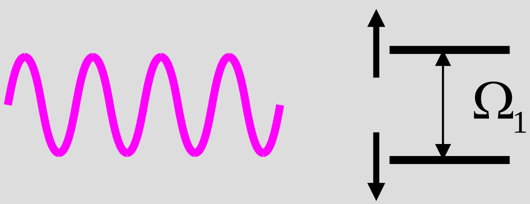
Quantum Mechanics of Superconducting Electrical Circuits

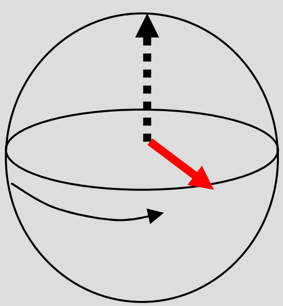


R. Schoelkopf group, Yale

NMR language

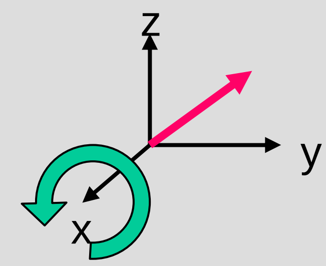
microwave pulse

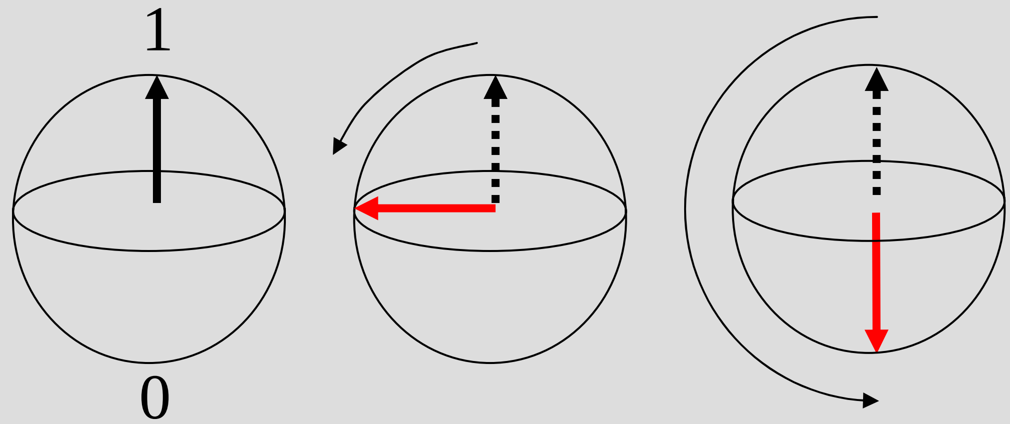




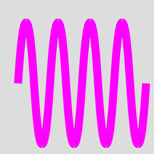
free evolution (analogous to gyroscopic precession)

Quantum control of qubits



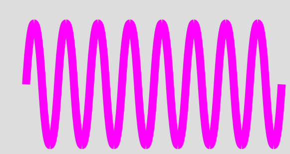


π/2
pulse



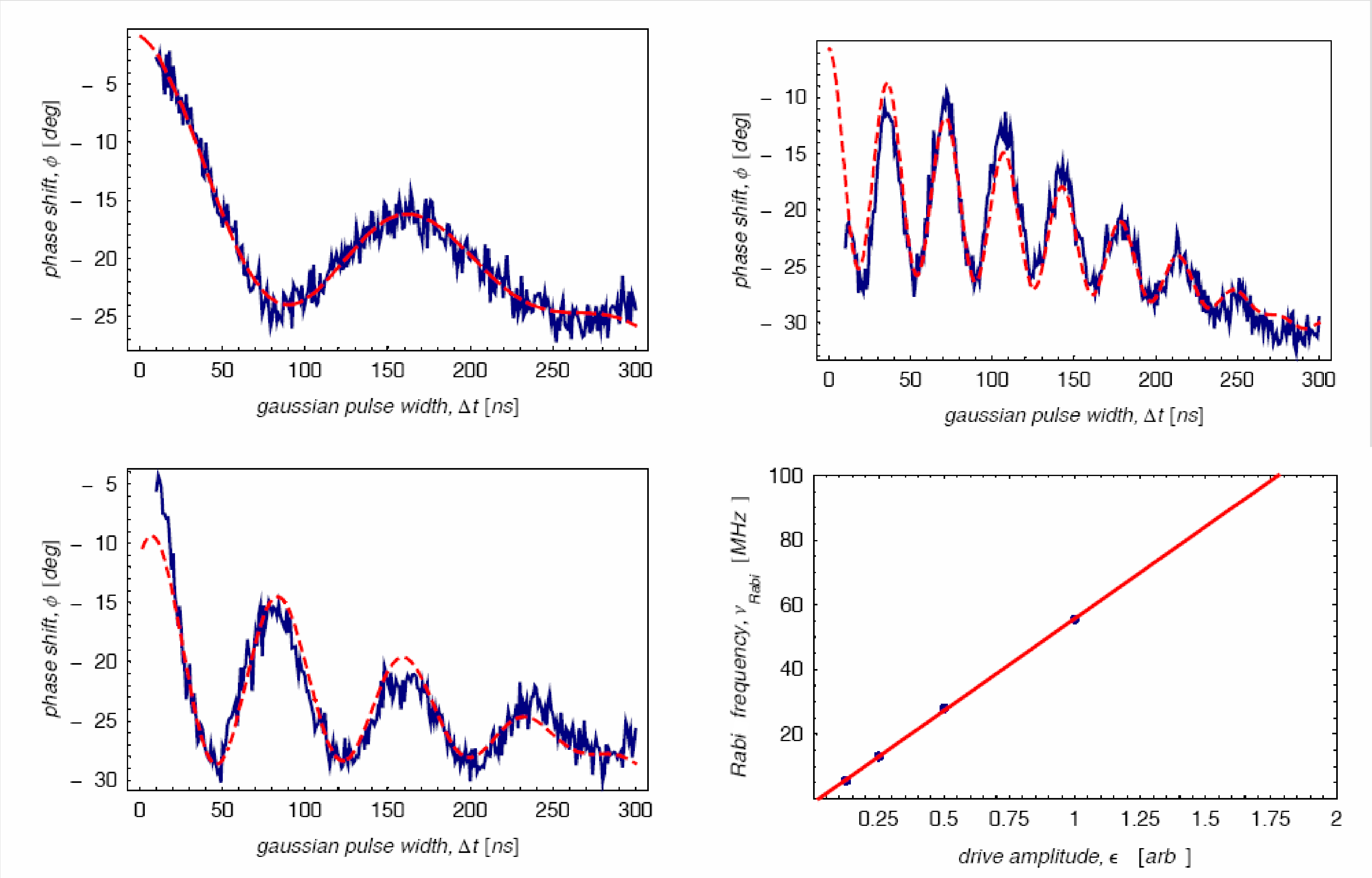
$\sqrt{\text{NOT}}$

π
pulse



NOT

Rotating the Qubit Orientation
followed by Z measurement



"Where a calculator on the ENIAC is equipped with 18,000 vacuum tubes and weighs 30 tons, computers in the future may have only 1,000 vacuum tubes and perhaps only weigh one and a half tons."

Popular Mechanics, 1949

Many thanks to: Ren-Shou Huang, Alexandre Blais, Krishnendu Sengupta, Aash Clerk, Doug Stone, Andreas Wallraff, David Schuster, Robert Schoelkopf, Michel Devoret

We still have a long way to go.

Theorist

Experimentalist

References

http://pantheon.yale.edu/~smg47

http://research.yale.edu/boulder

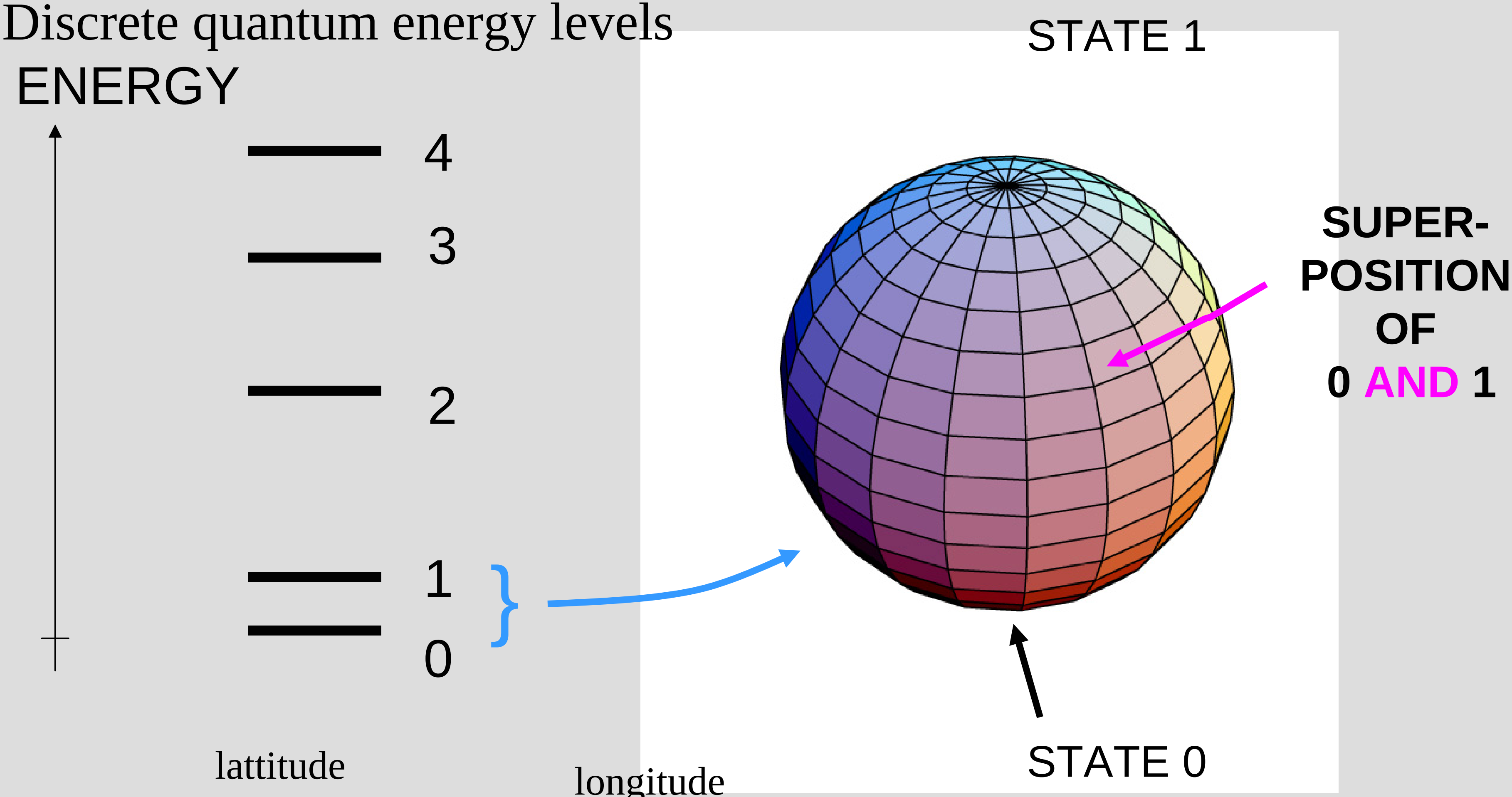
http://cam.qubit.org

http://www.theory.caltech.edu/people/preskill

The End

ELEMENTARY QUANTUM INFORMATION UNIT: QUBIT

Discrete quantum energy levels



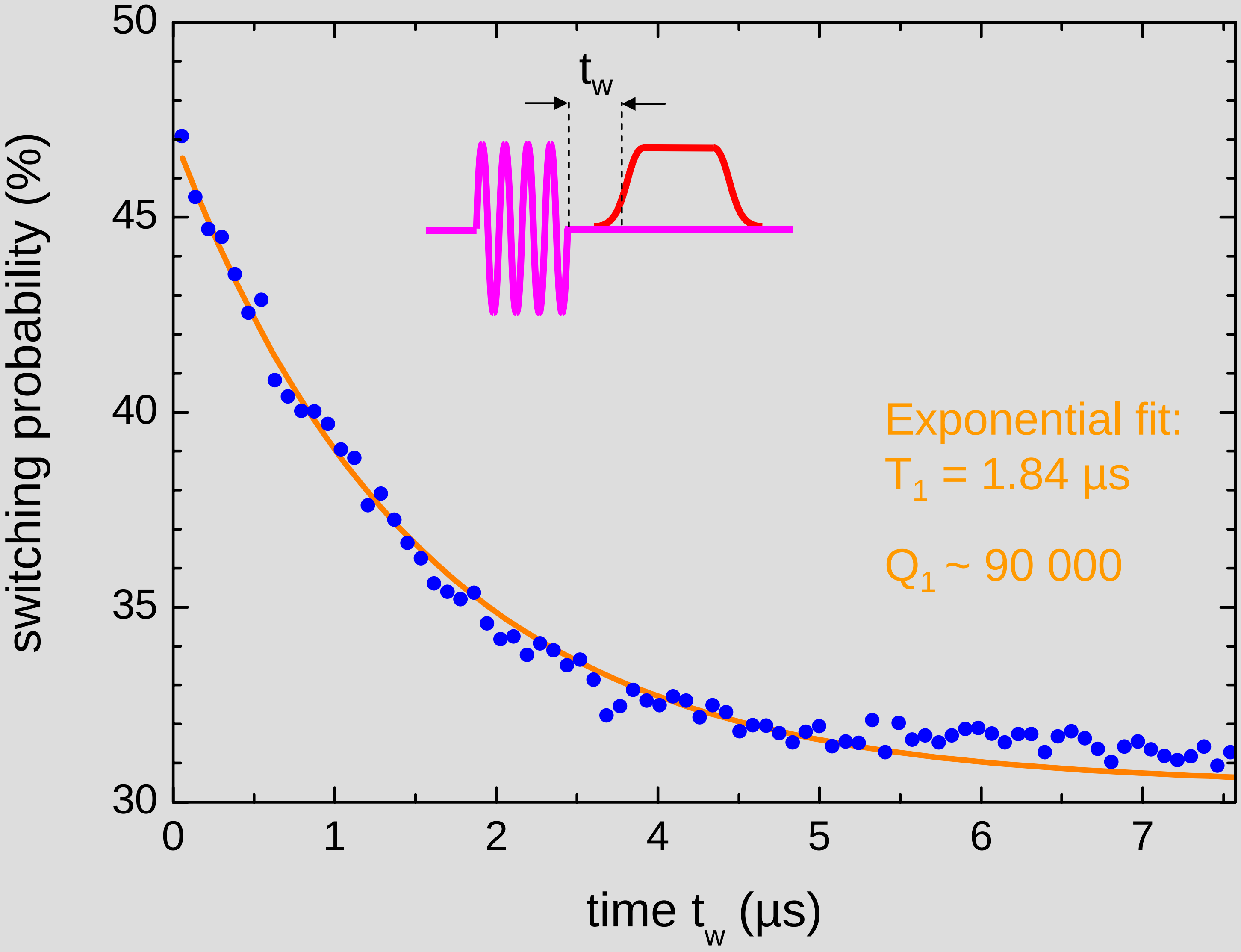
lattitude

longitude

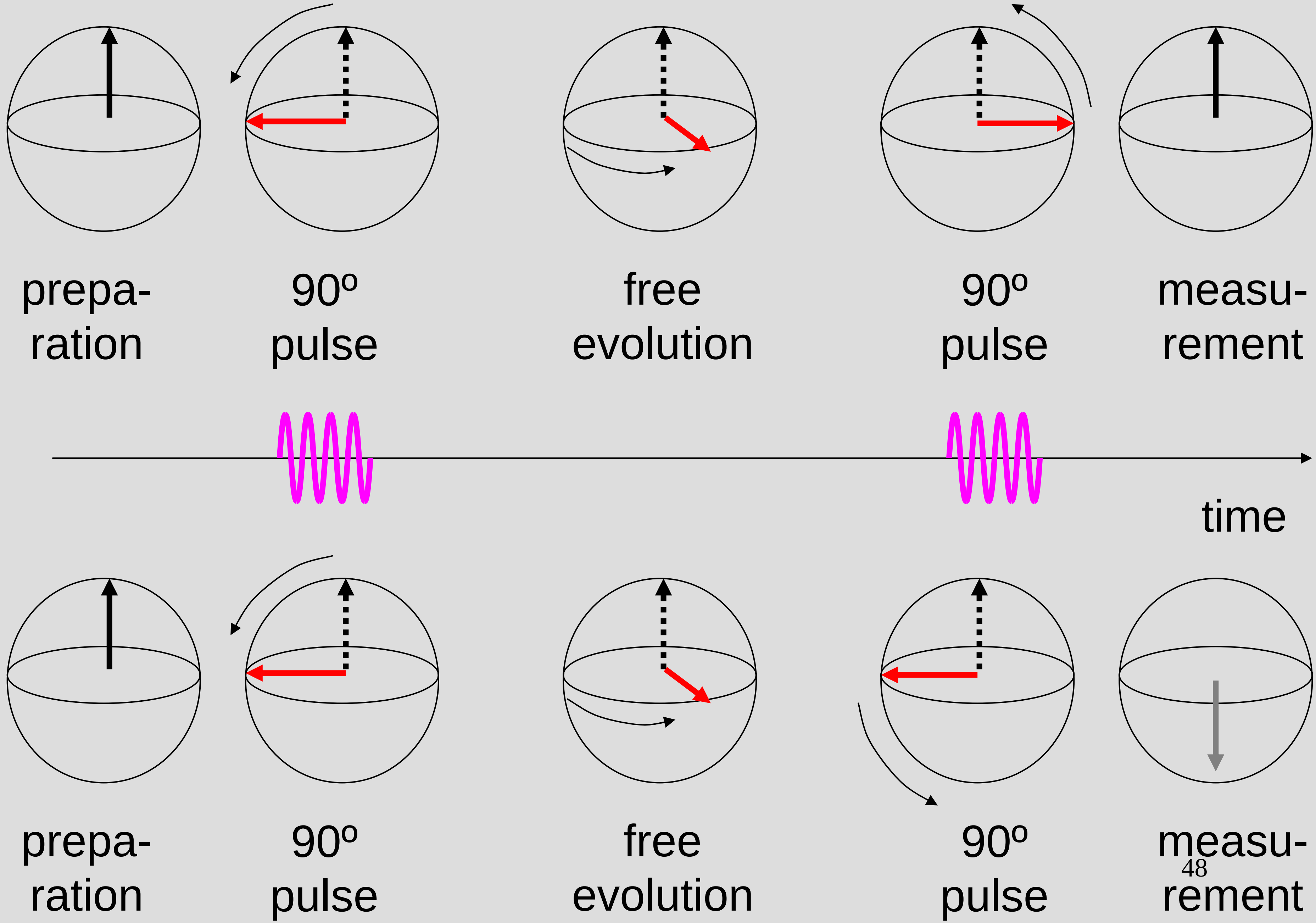
$$|\psi\rangle = \cos(\theta/2)|1\rangle + e^{i\varphi}\sin(\theta/2)|0\rangle$$

Courtesy M. Devoret

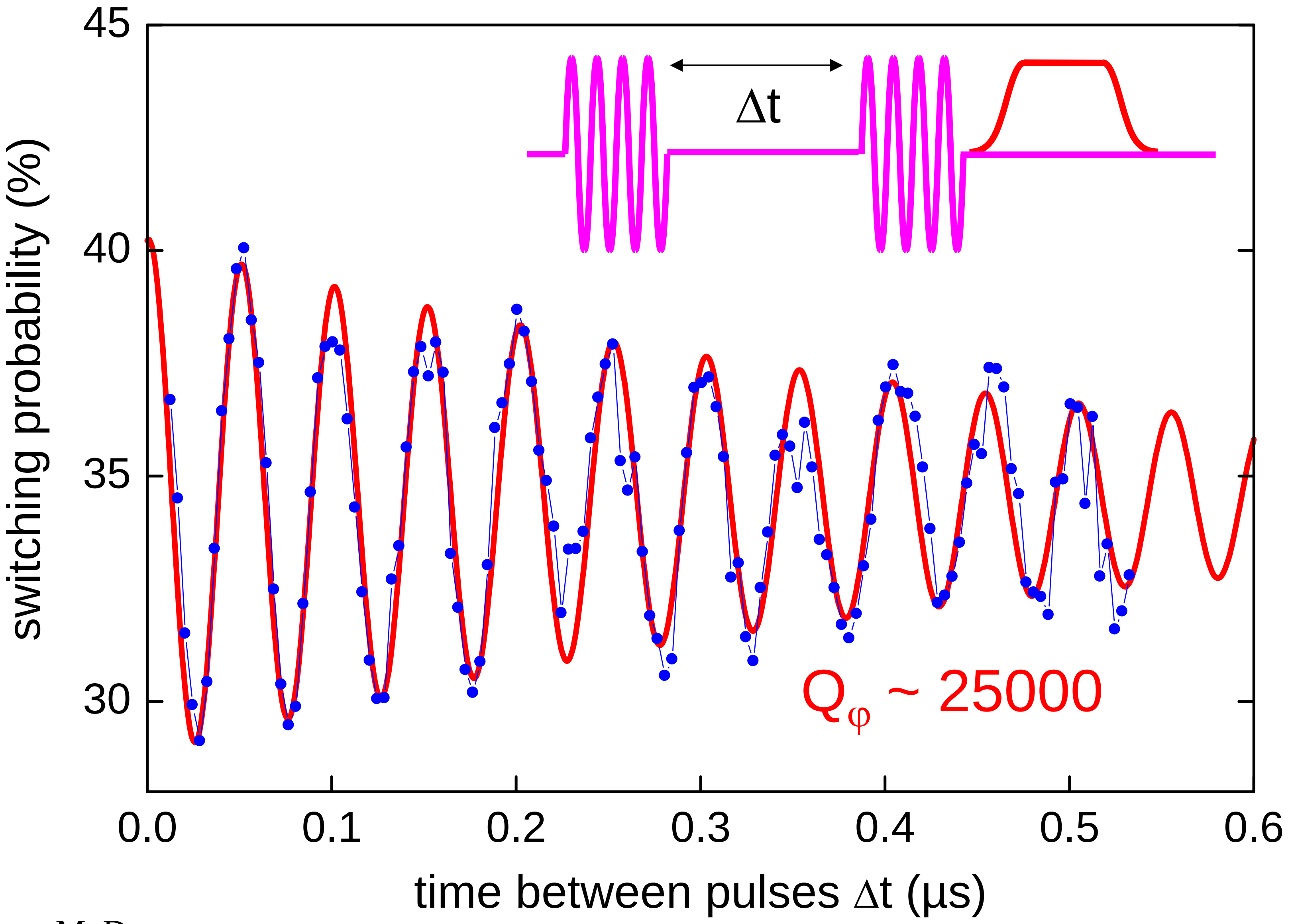
RELAXATION TIME AT OPTIMAL POINT



PRINCIPLE OF RAMSEY EXPERIMENT



RAMSEY FRINGES



Courtesy M. Devoret

Summary and Conclusions

- Quantum parallelism is powerful but difficult
- Algorithms are limited
- Engineering issues:
  - -decoherence, fidelity of operations
  - -isolation, interaction, readout of qubits
  - -scalability to large sizes
- Quantum control of single solid state qubits has been demonstrated for the first time
  - -10^4 Ramsey fringes; $T_1 \sim 2\,\mu s$; $T_2 \sim 0.5\,\mu s$
- Two-bit gates now in progress

Many thanks to:
Michel Devoret, Rob Schoelkopf
Aashish Clerk, Ren-shou Huang, K. Sengupta

Special thanks to Michel Devoret for several of the transparencies.

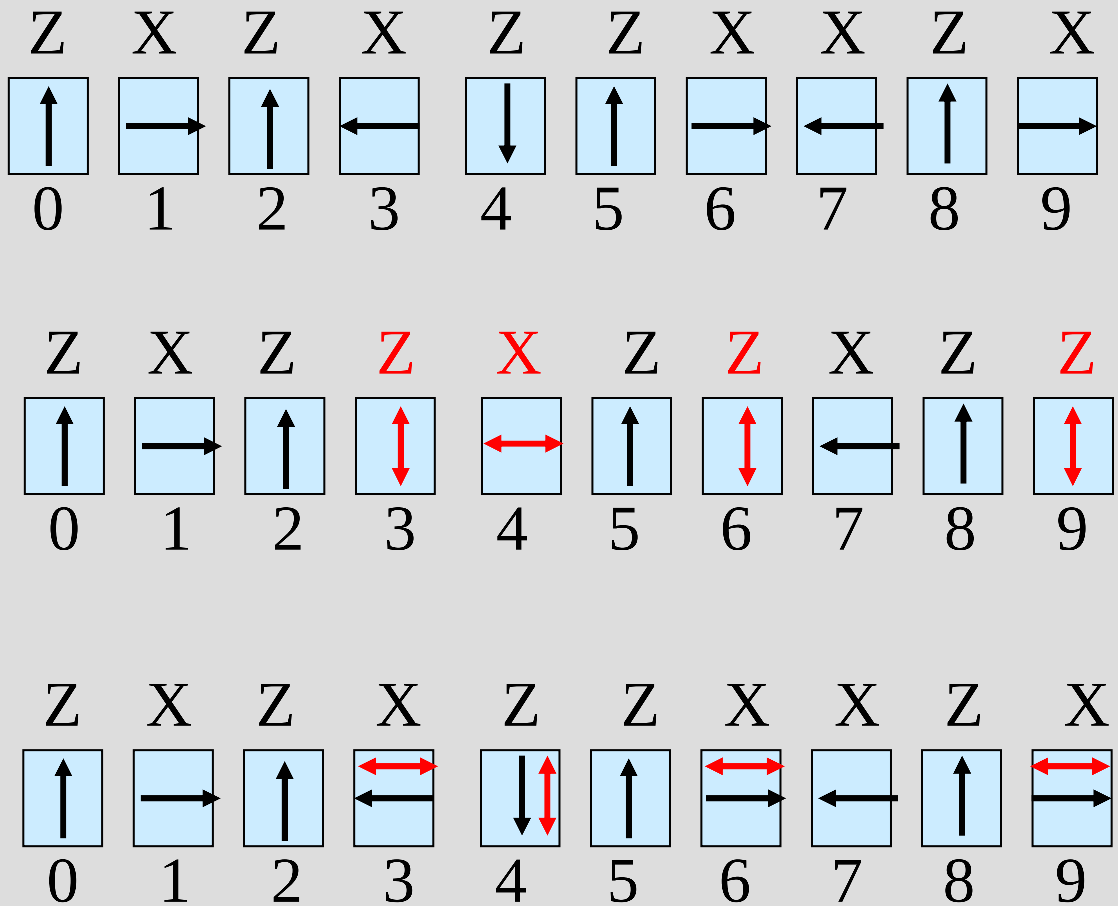
When it comes to quantum mechanics you have to think different

What the counterfeiter sees

Original:

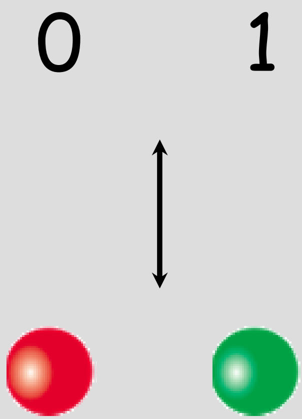
As seen and cloned by counterfeiter:

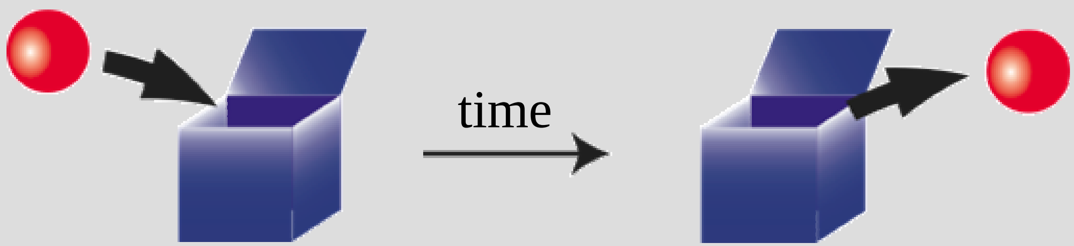
Clone as seen by govt. inspector



$$P_{\text{match}} = \left(3/4\right)^{n} = 0.056 \quad \text{for } n = 10.$$

Fundamental features of classical information:



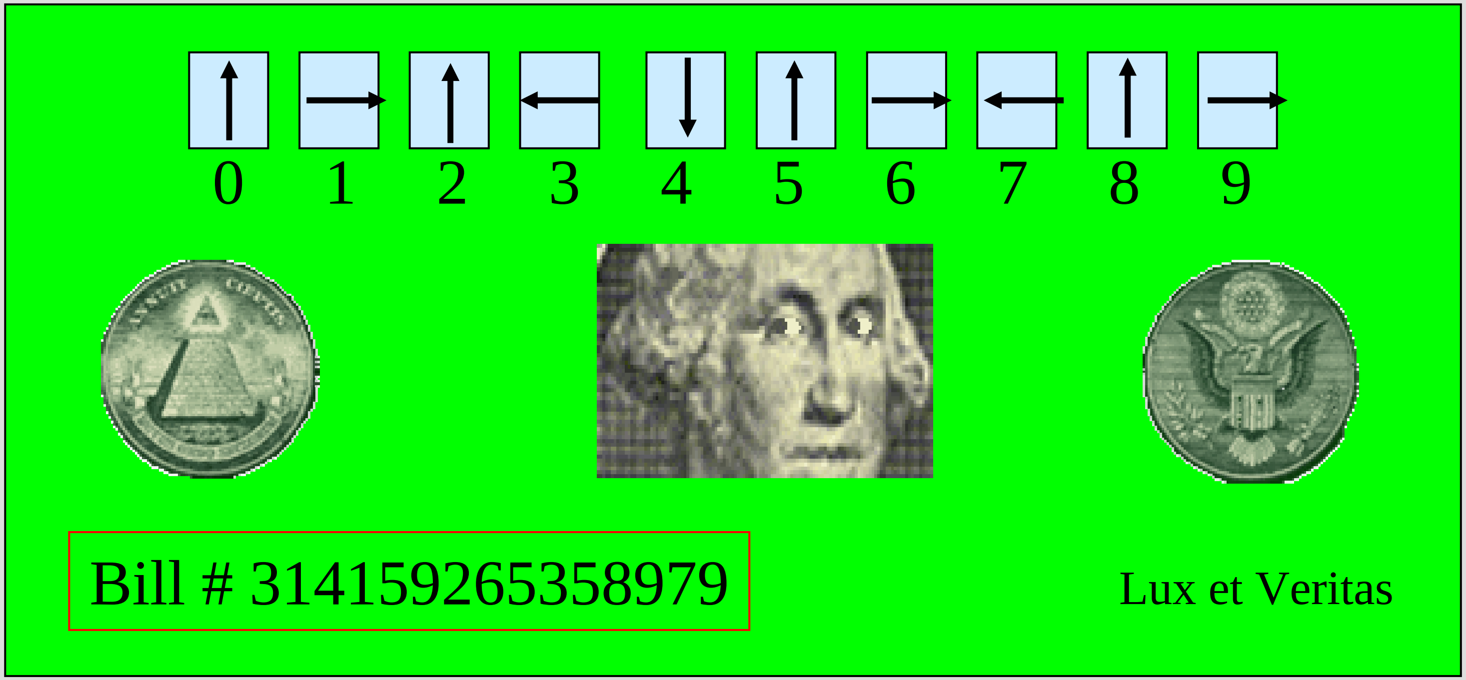


Classical Information:

- Easily stored and read out
- Easily copied

(A. Blais after J. Preskill)

Is it Counterfeit?



Government issue detector orientations for this bill
(kept in a secret book by the Treasury Department)