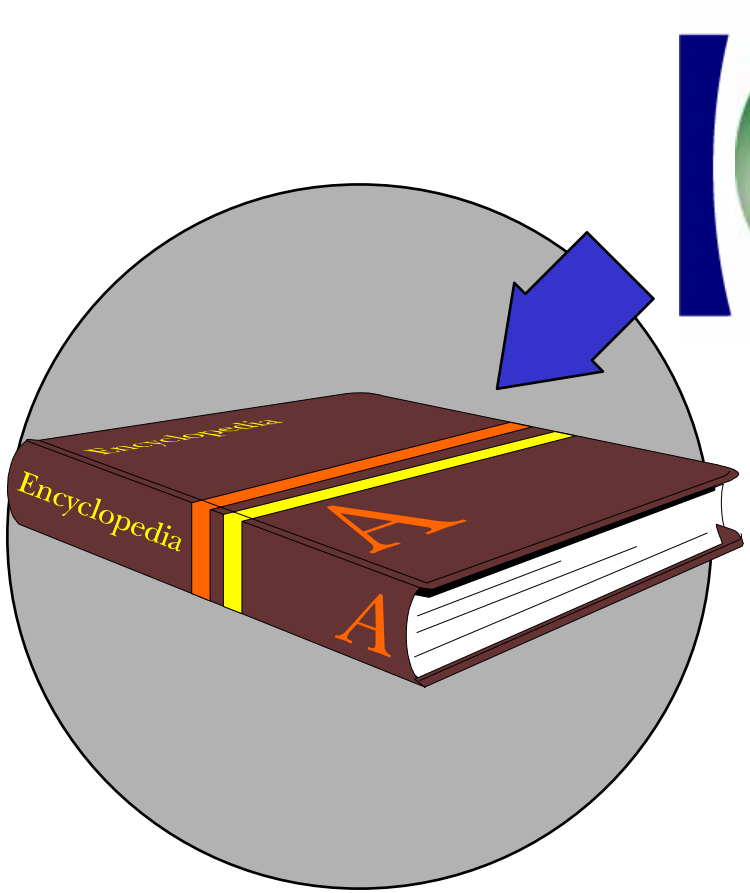
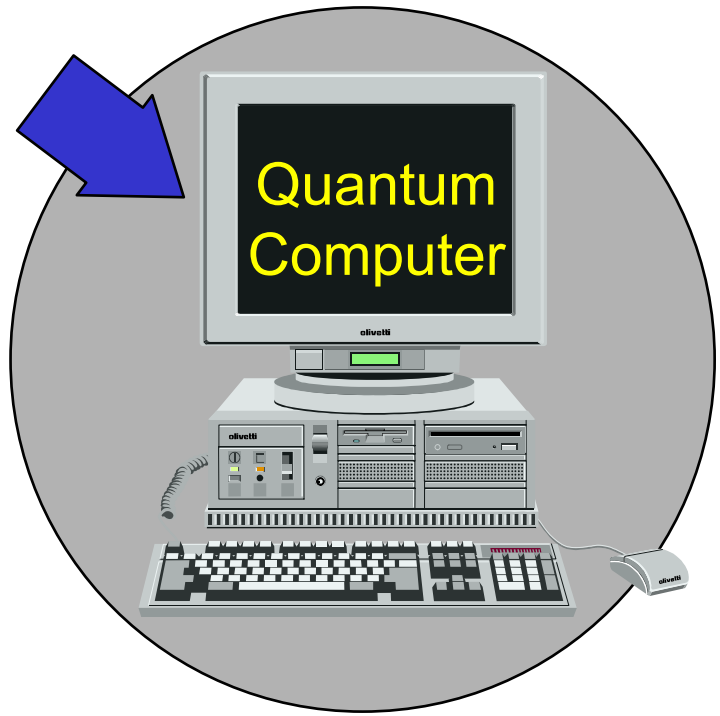
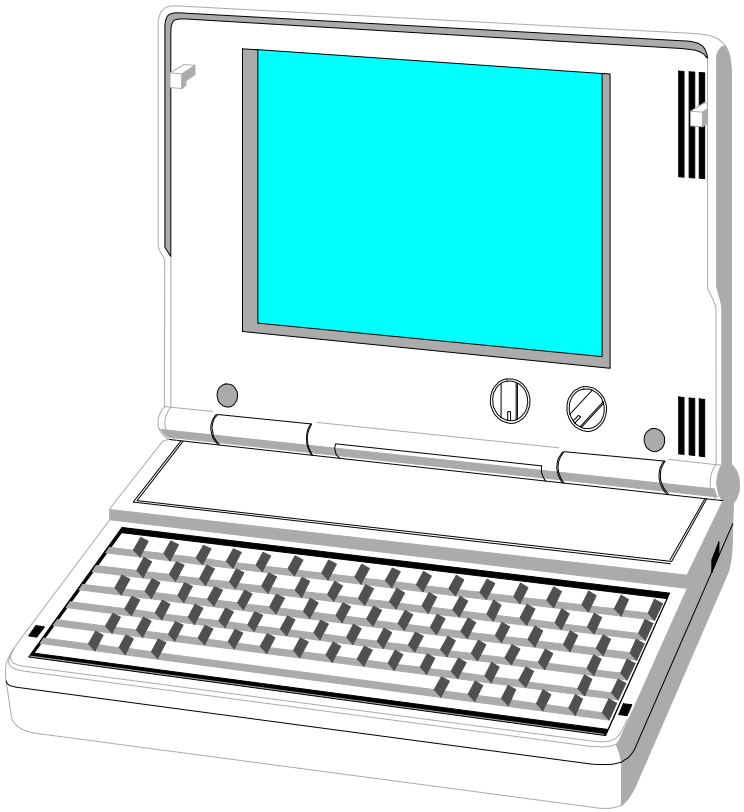
Putting Weirdness to Work: Quantum Information Science



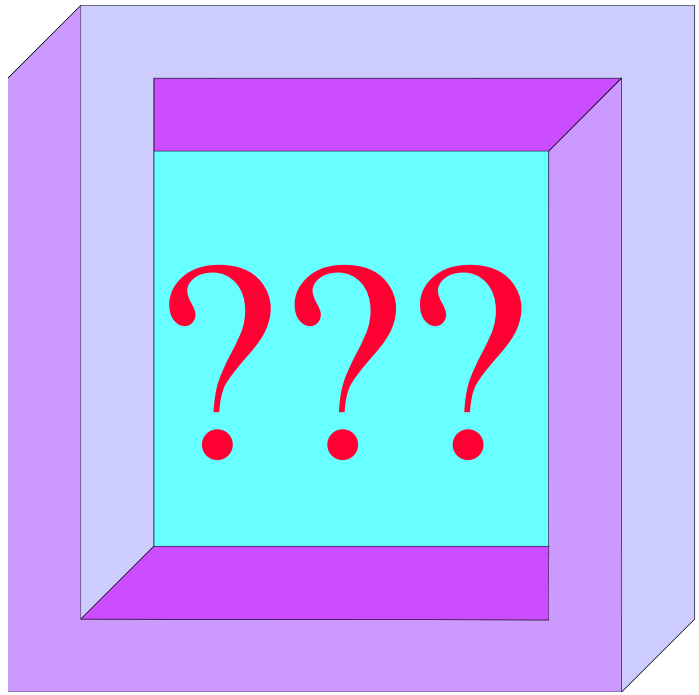


John Preskill, Caltech
KITP Public Lecture
3 May 2006

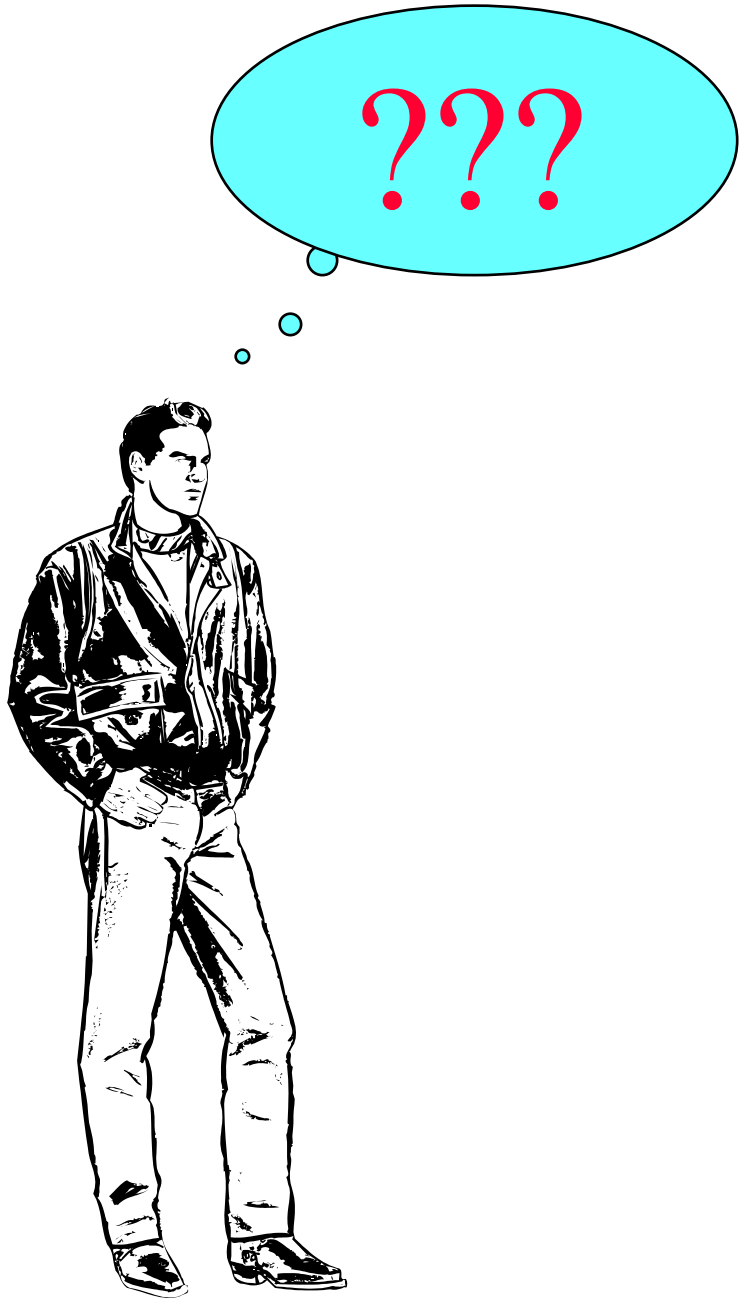
IQI Institute for Quantum Information
Sponsored by the NSF

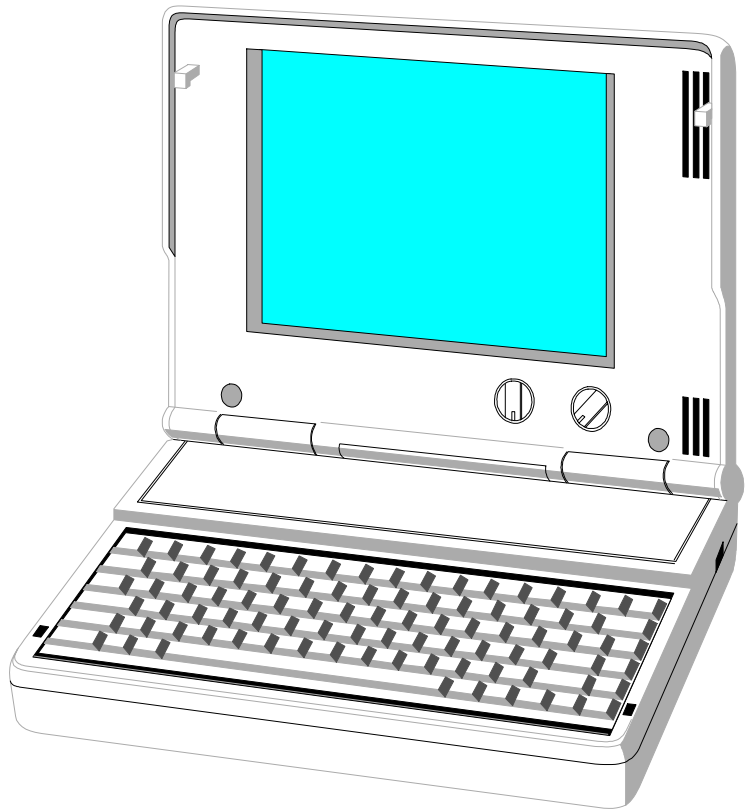


2006



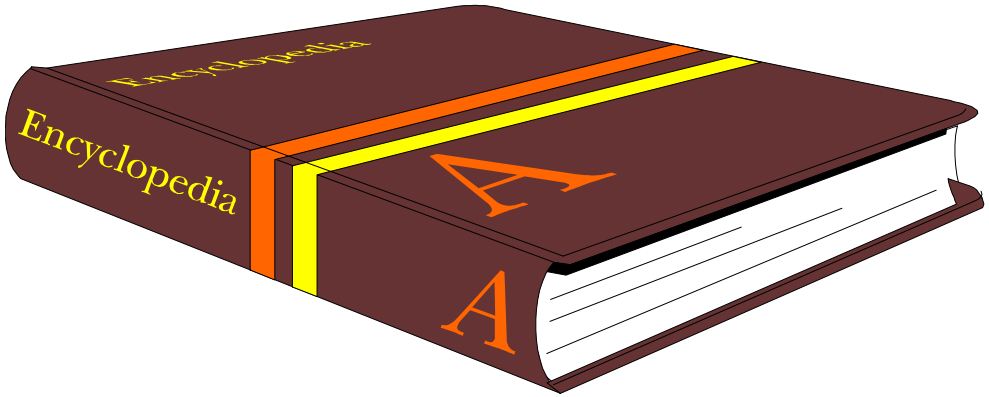
2100





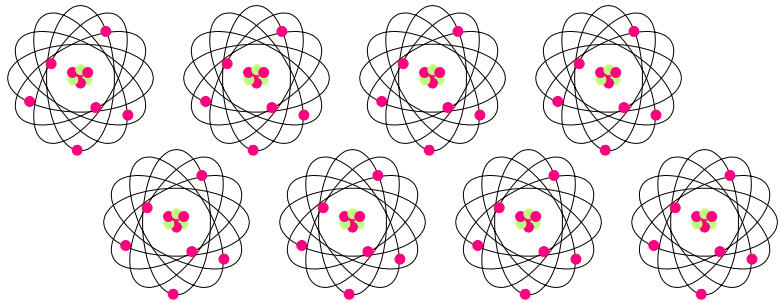
2006


Quantum
Theory
Q



Information

is encoded in the state of a *physical* system.



Information

is encoded in the state of a *quantum* system.

Theoretical Quantum Information Science

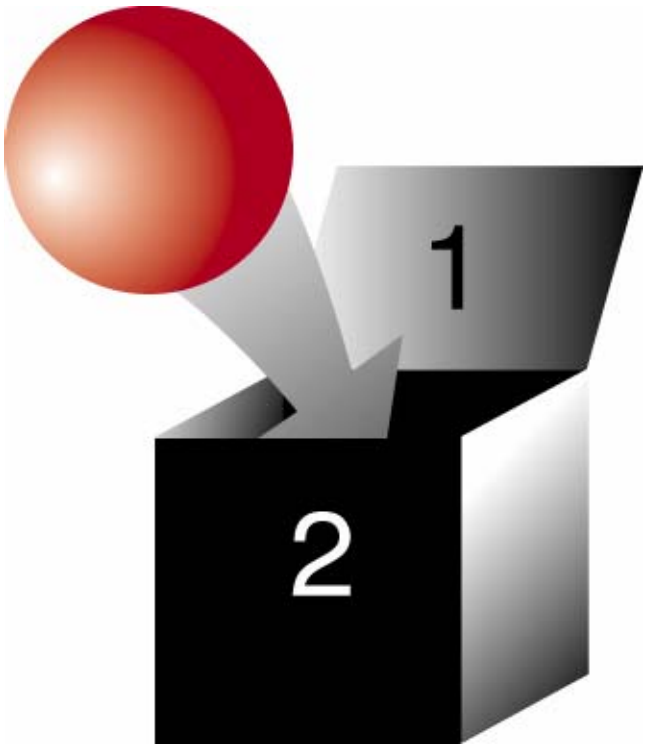
is driven by ...

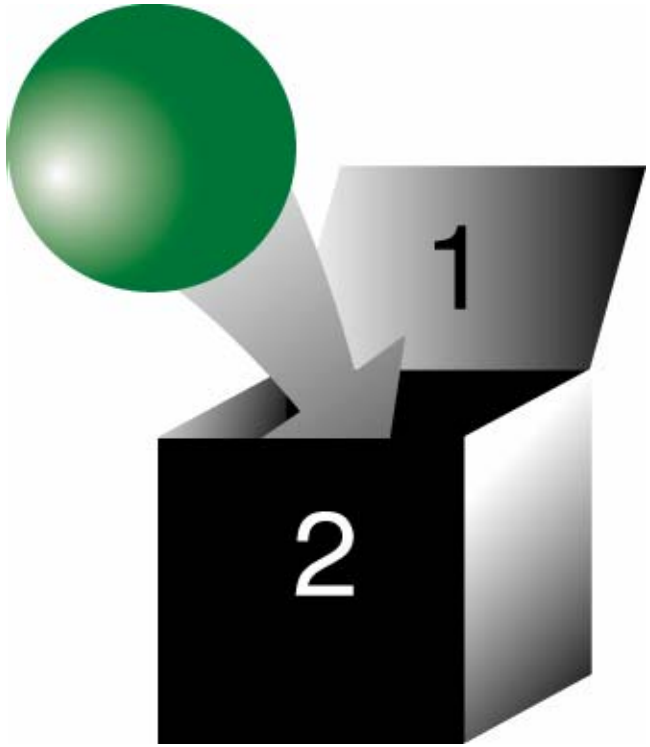
Three ***Great*** Ideas:

1) Quantum Cryptography
2) Quantum Computation
3) Quantum Error Correction

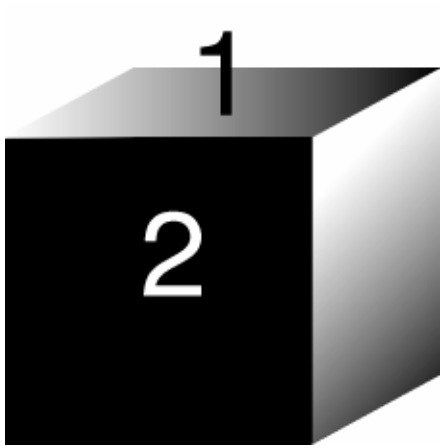
Though quantum theory is over 100 years old, these ideas have begun to draw substantial attention in just the past few years.

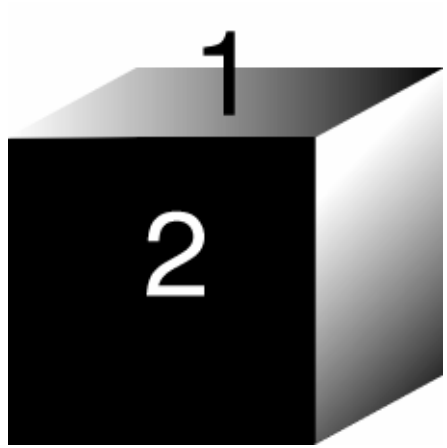
Classical Bit



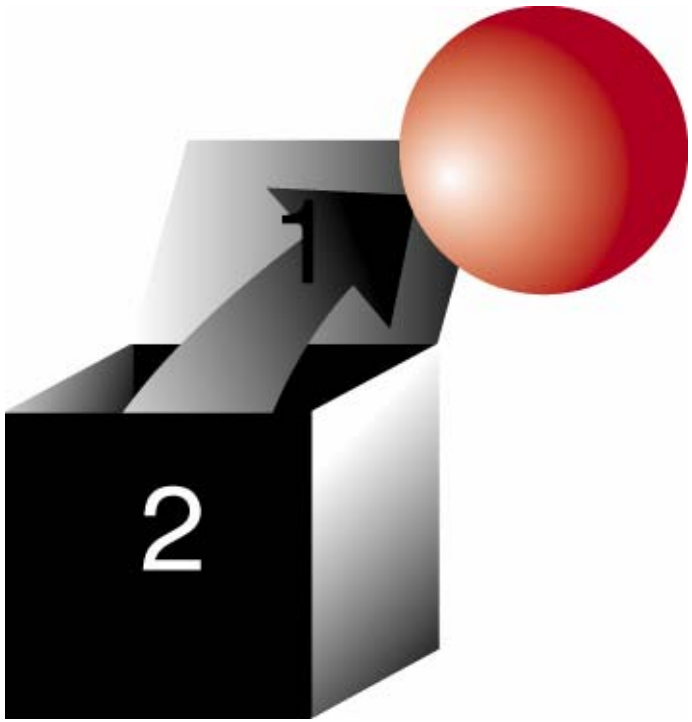


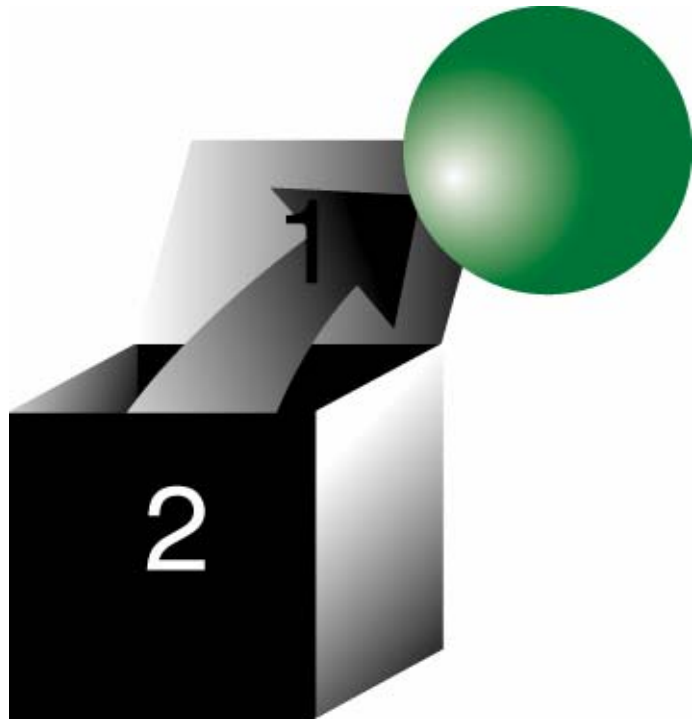
Classical Bit





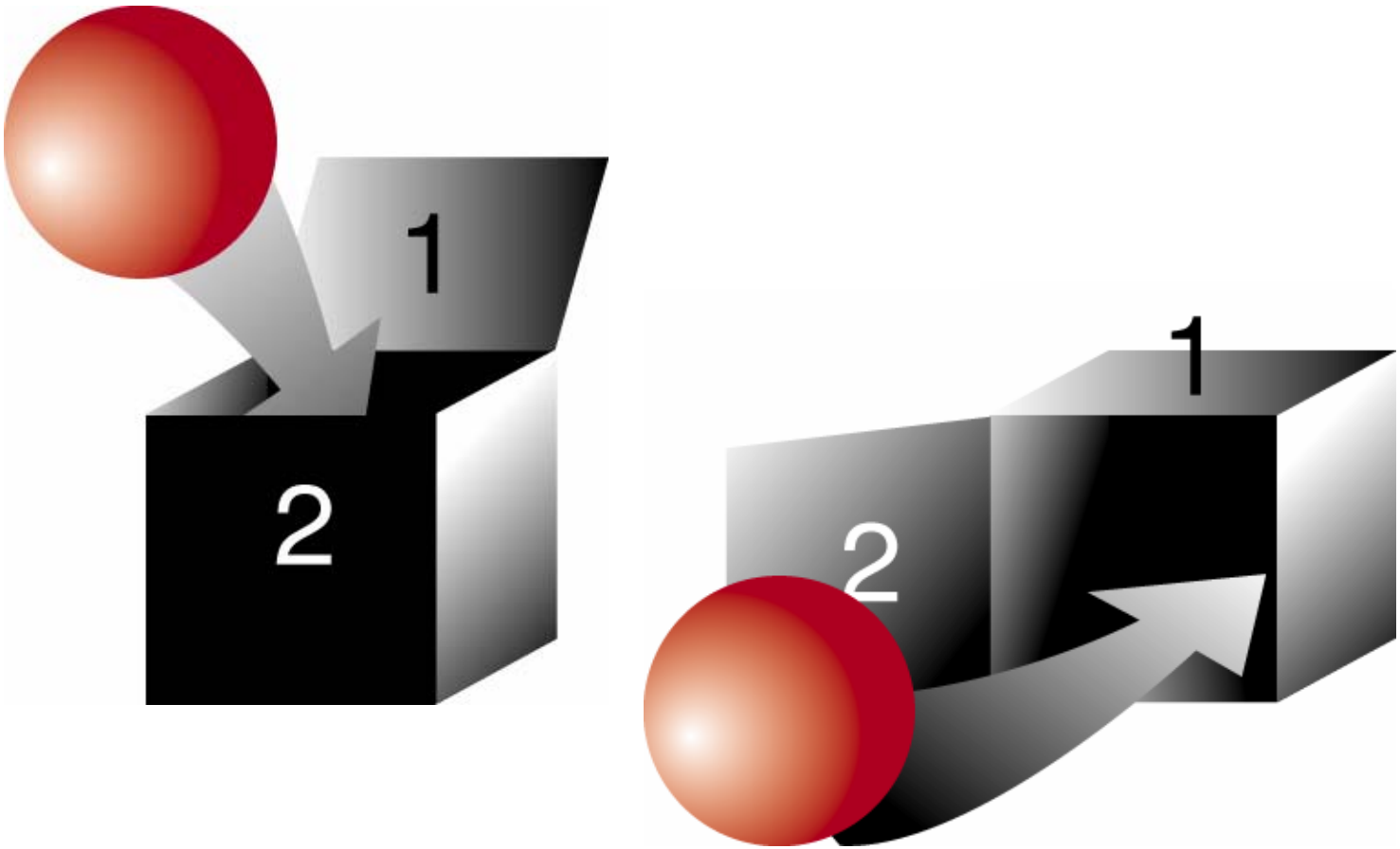
Classical Bit





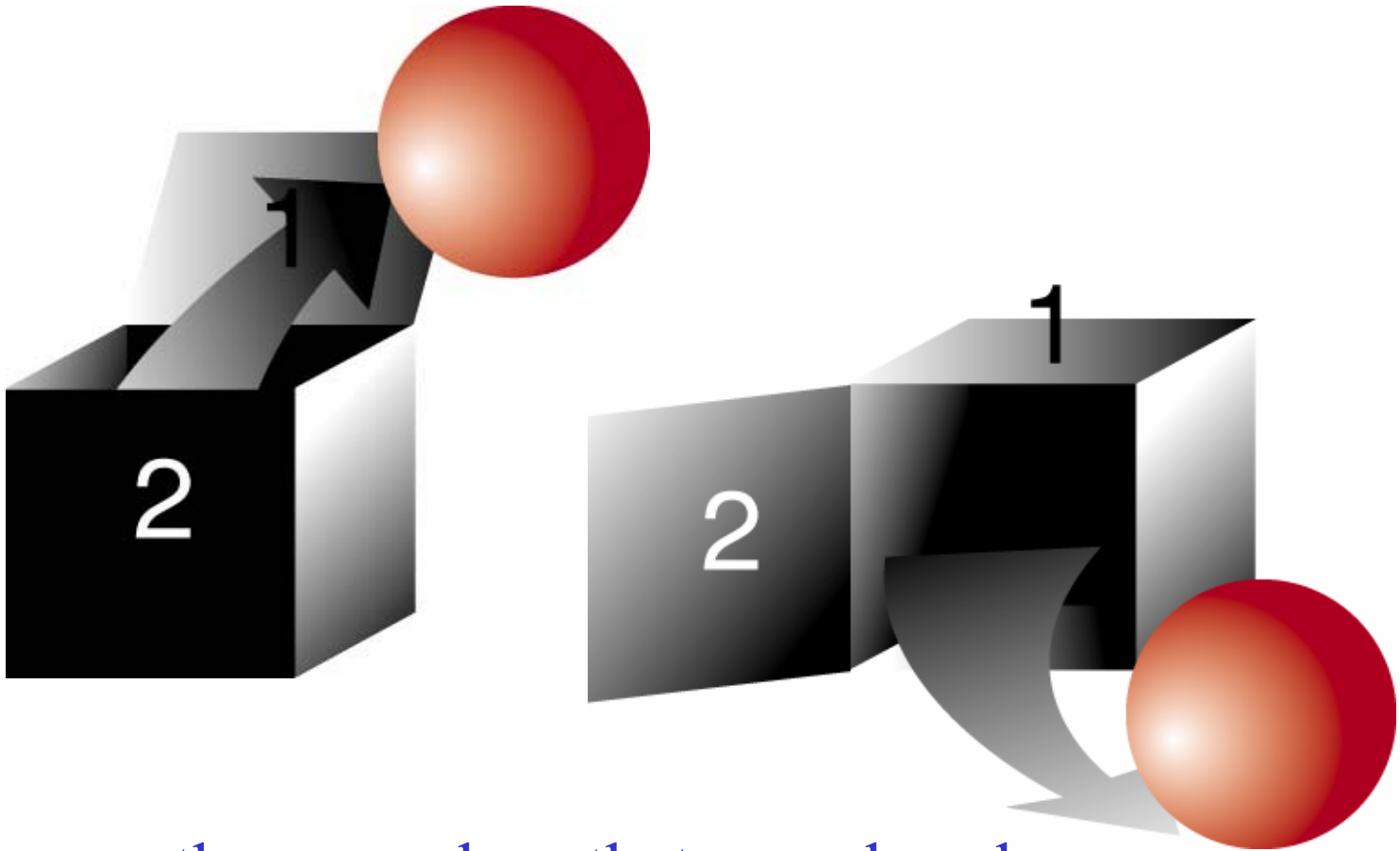
What went in, comes out.

Quantum Bit ("Qubit")



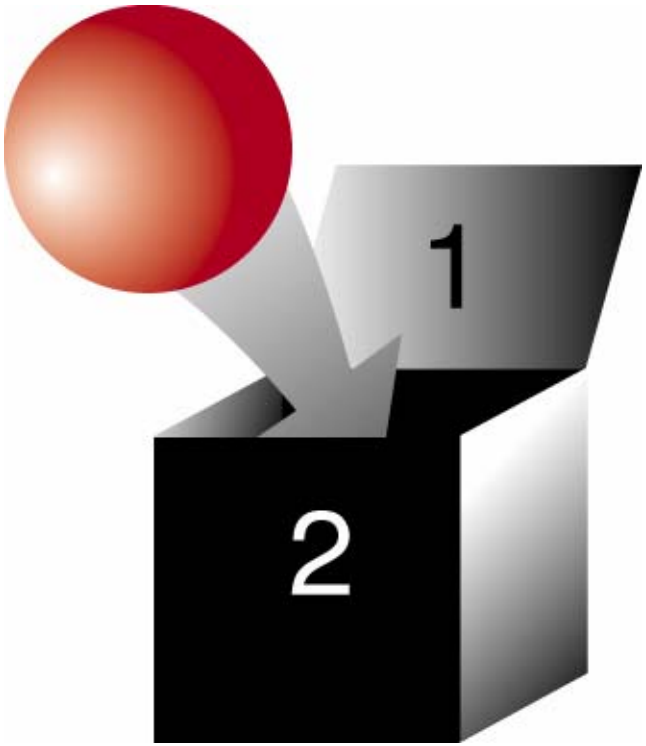
The two doors are two different ways to prepare or measure the quantum state of an atom or photon (but never mind).

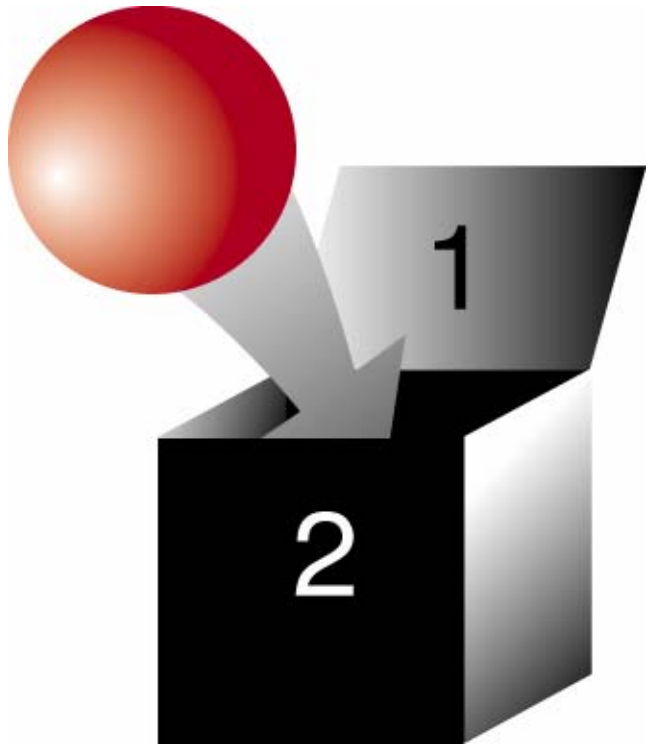
Quantum Bit ("Qubit")



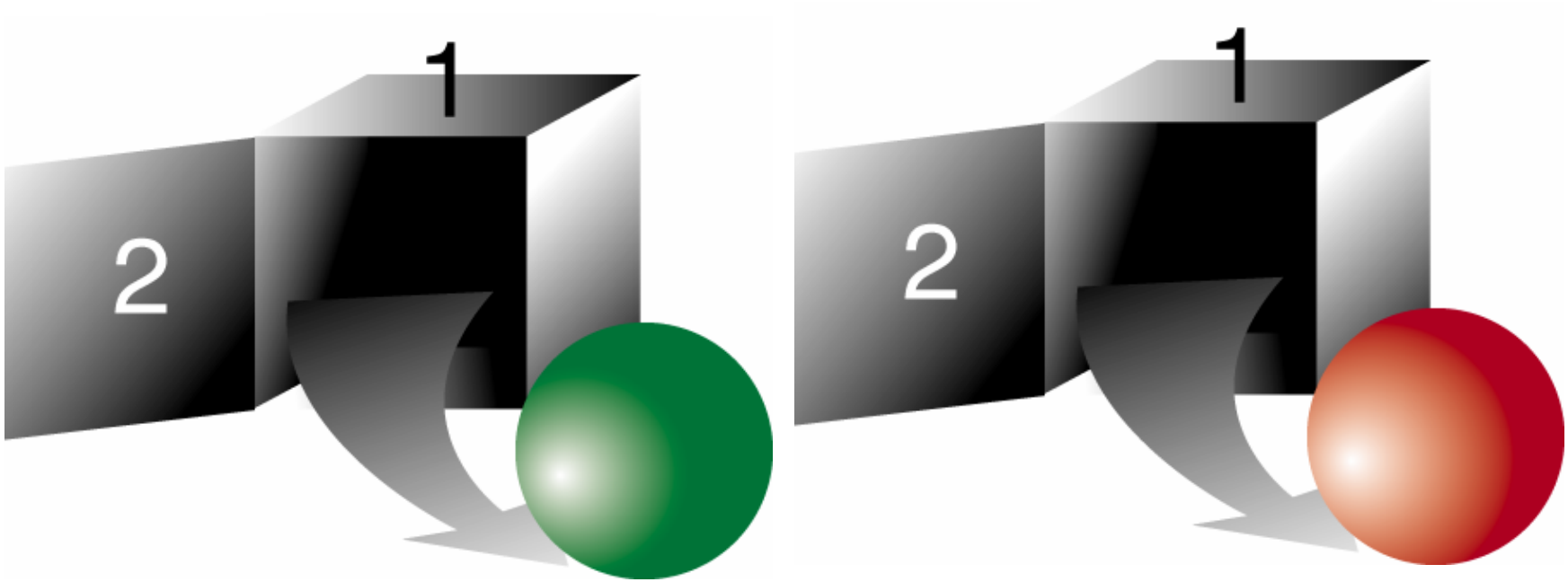
If you open the *same* door that you closed,
you can recover the bit from the box.

Quantum Bit (“Qubit”)



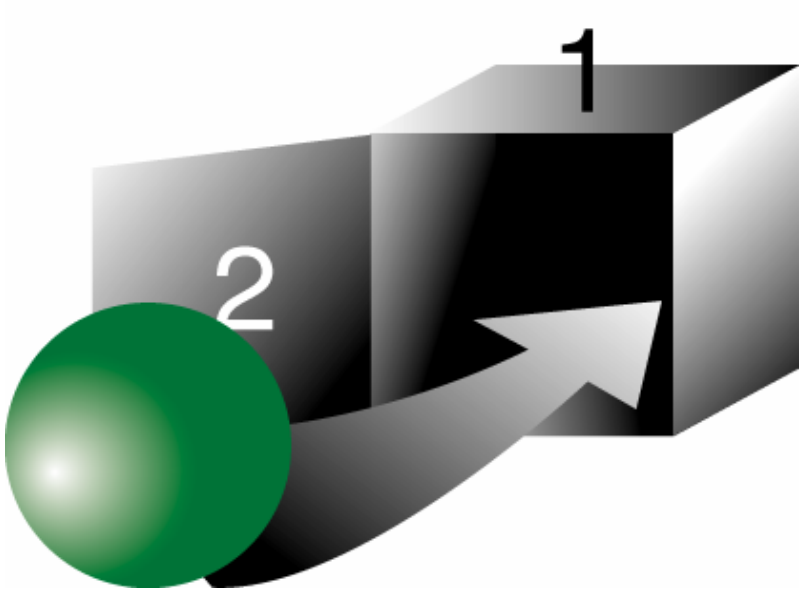


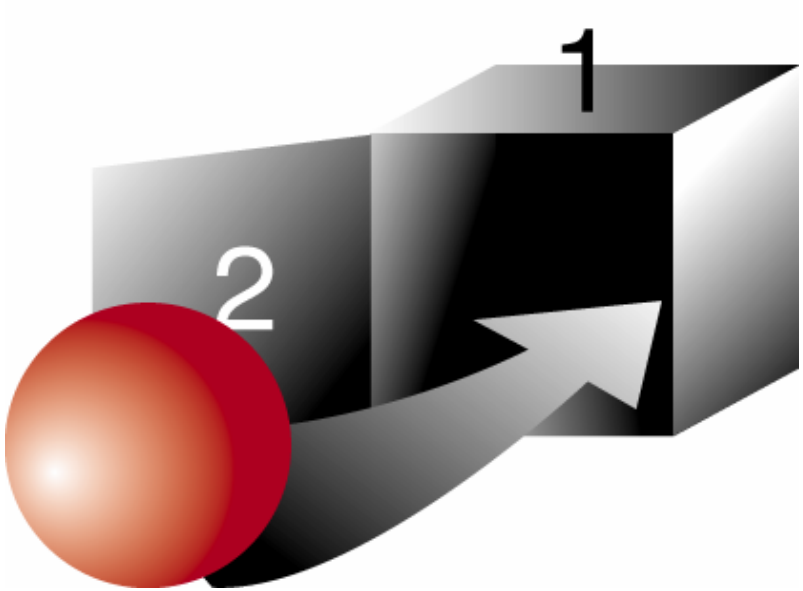
Quantum Bit ("Qubit")



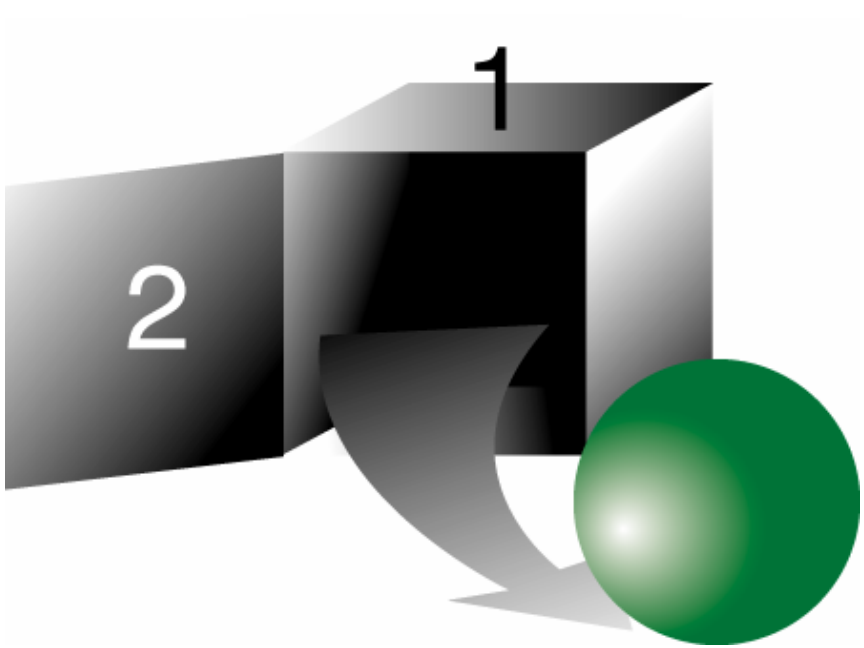
If you open a *different* door than you closed, the color is *random* (red 50% of the time and green 50% of the time).

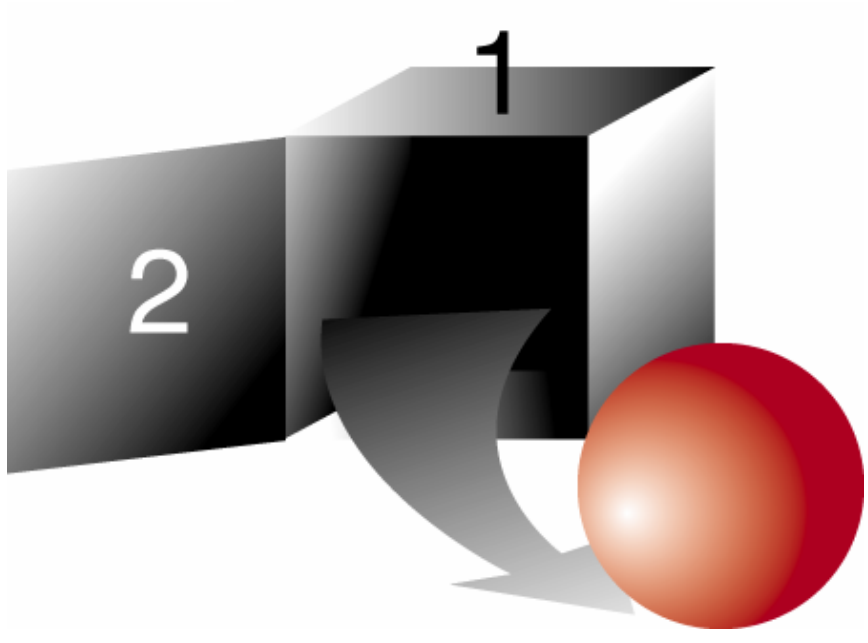
Quantum Bit (“Qubit”)





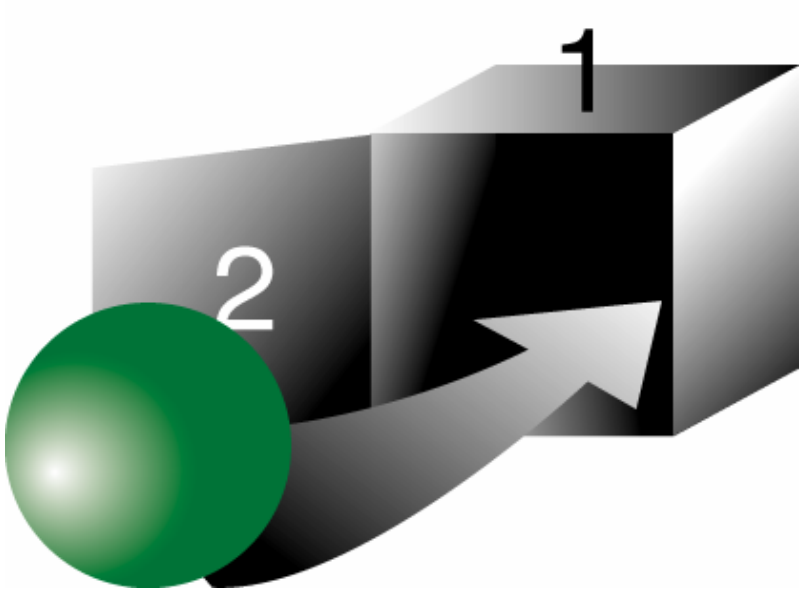
Quantum Bit ("Qubit")

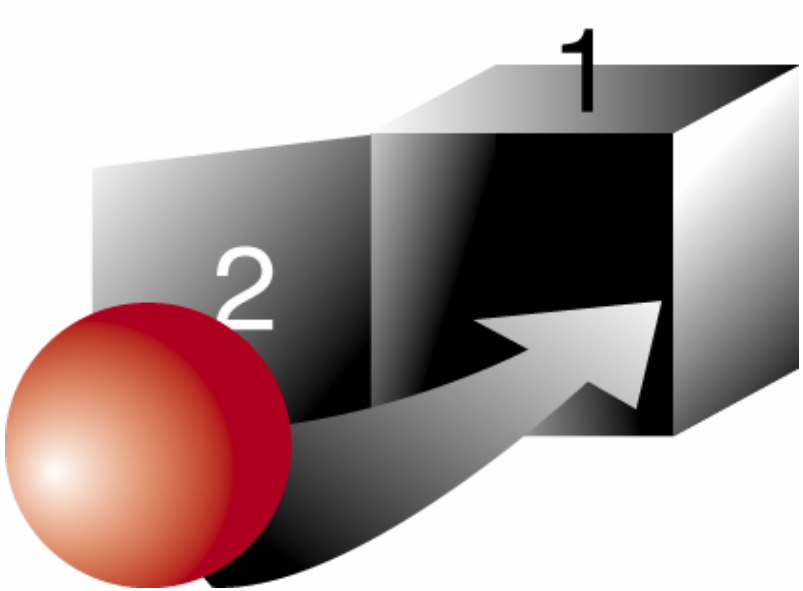




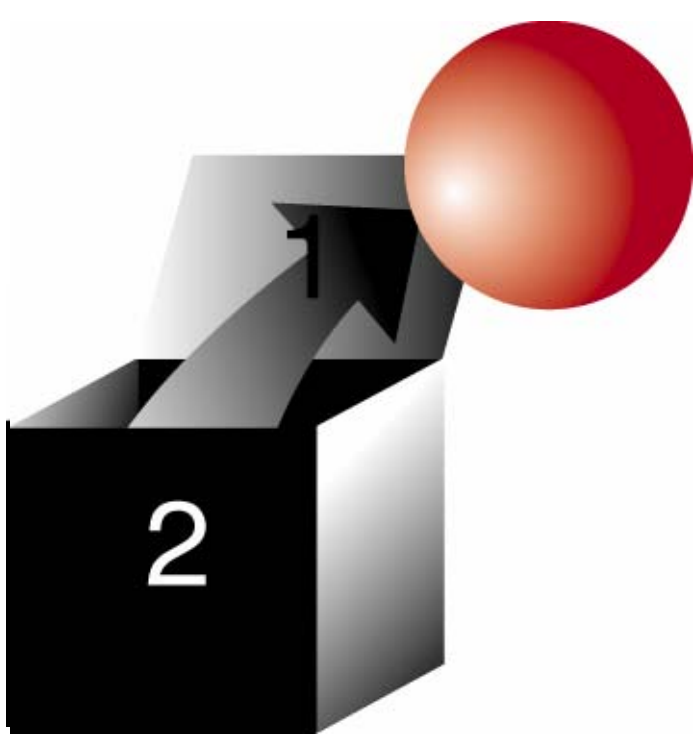
If you open the *same* door that you closed,
you can recover the bit from the box.

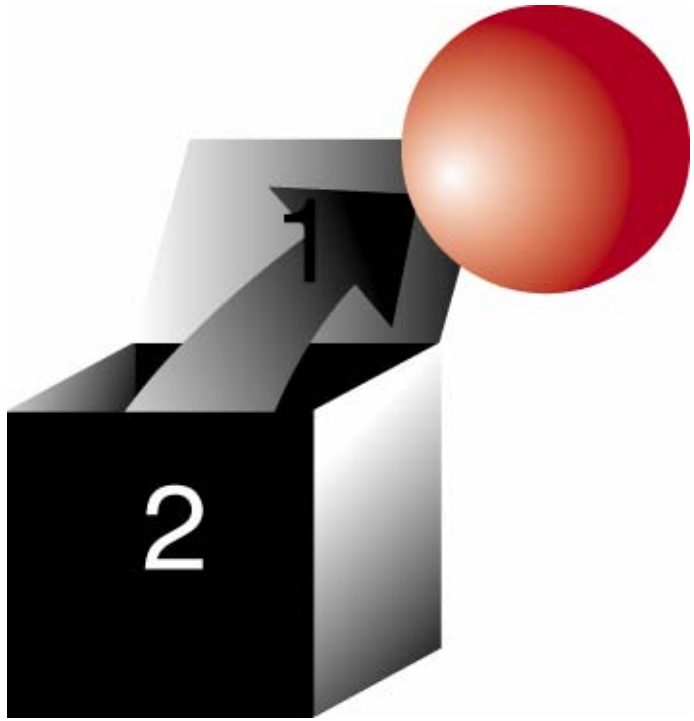
Quantum Bit (“Qubit”)



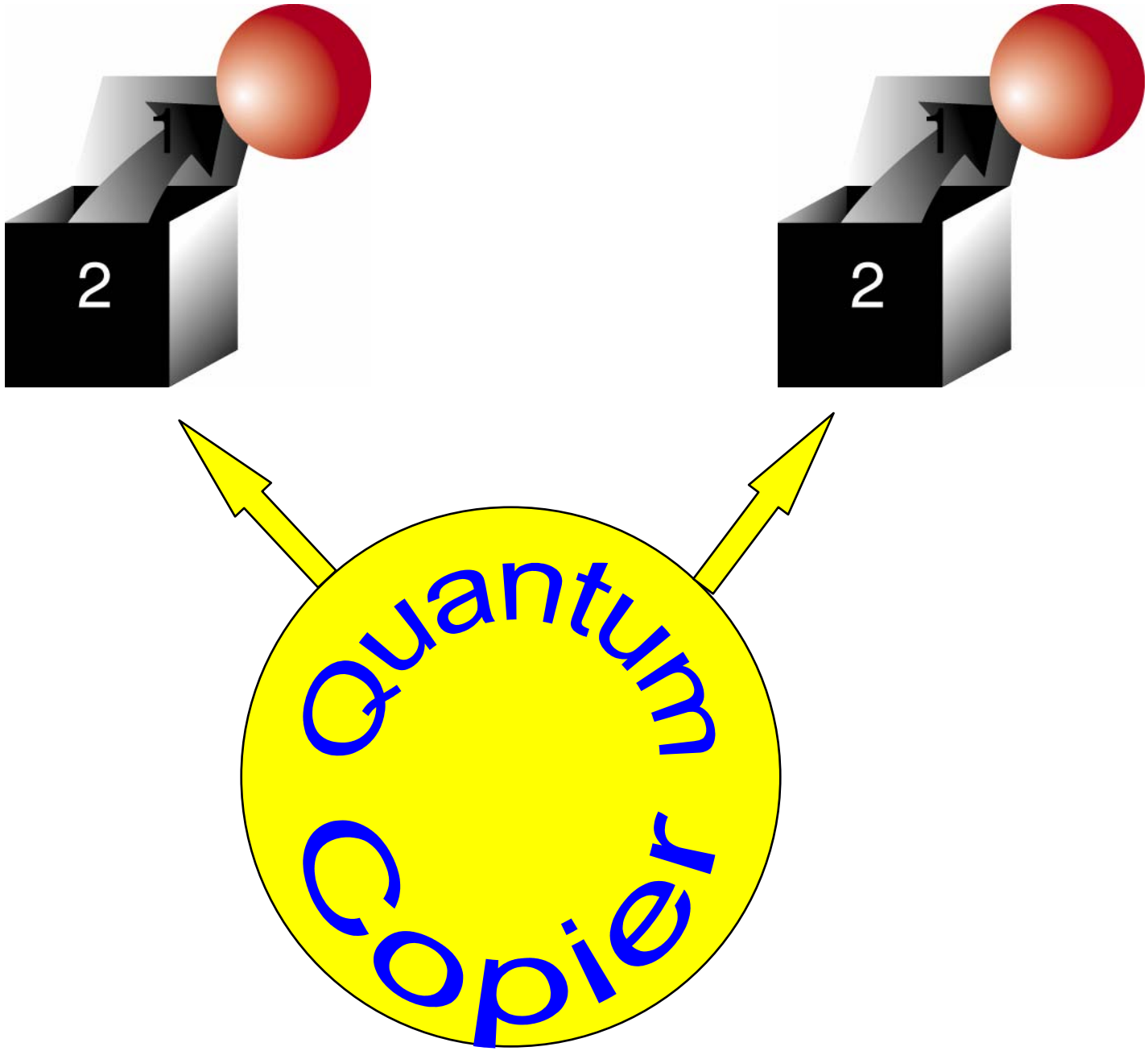


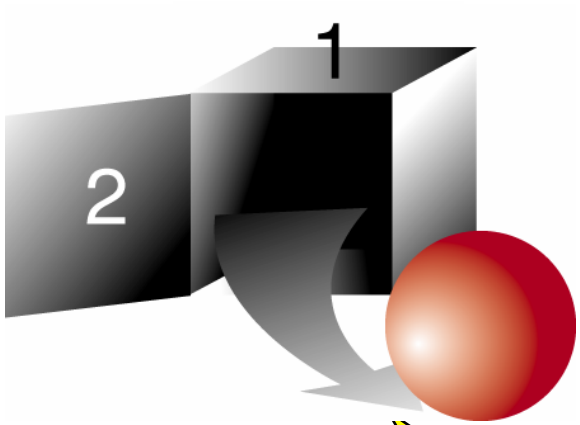
Quantum Bit ("Qubit")

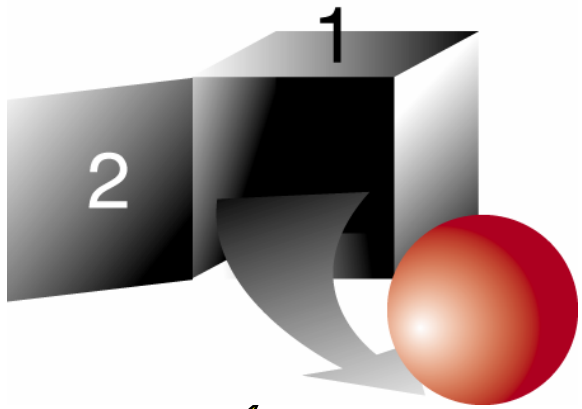


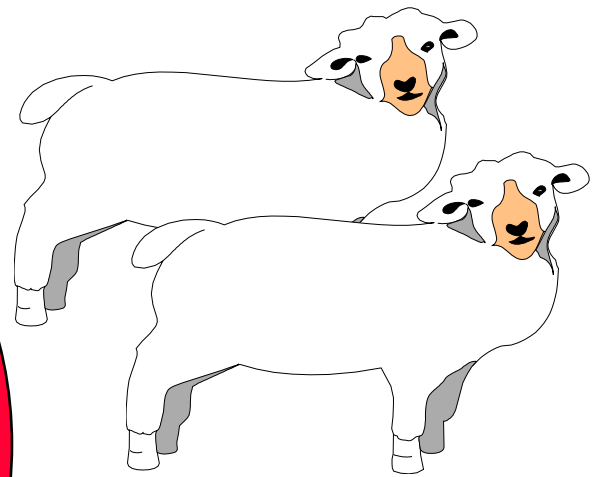


If you open a *different* door than you closed, the color is *random* (red 50% of the time and green 50% of the time).


1
2
1
2
Quantum
Copier

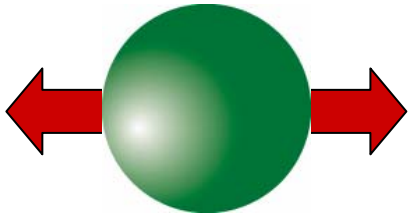




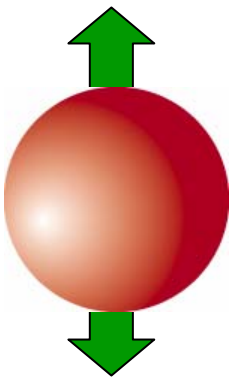


No cloning!

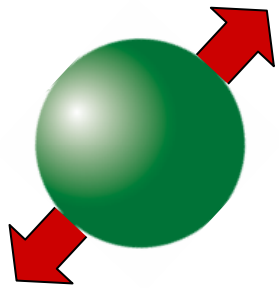
Photon polarization as a qubit



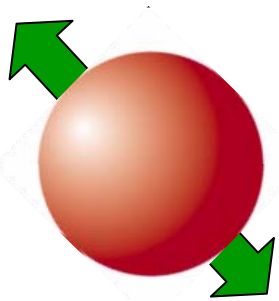
$= |0\rangle$



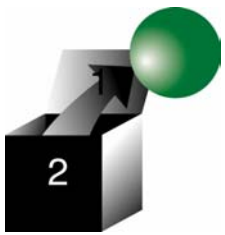
$= |1\rangle$

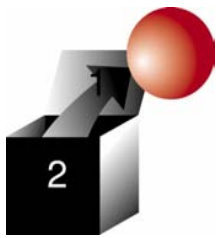


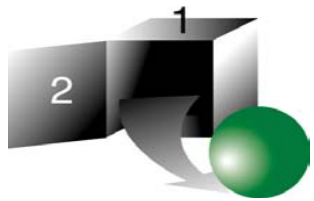
$= \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle \right)$

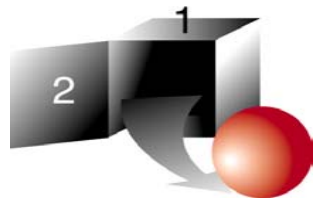


$= \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle \right)$









Alice

Eve

Bob

No tapping a quantum telephone!!

Alice

Eve

Bob

Unbreakable code: if Alice and Bob share a random key (string of bits) that is not known to Eve.

Alice

Eve

Bob

Message: HI BOB

01001000 01001001 00100000 01000010 01001111 01000010
01110100 10111001 00000101 10101001 01011100 01110100

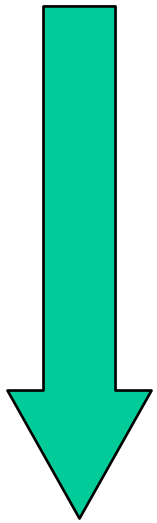
00111100 11110001 00100101 11101011 00010011 00110110

Alice

Message: HI BOB

01001000 01001001 00100000 01000010 01001111 01000010
01110100 10111001 00000101 10101001 01011100 01110100

Eve



Bob

00111100 11110001 00100101 11101011 00010011 00110110
01110100 10111001 00000101 10101001 01011100 01110100

01001000 01001001 00100000 01000010 01001111 01000010

HI BOB

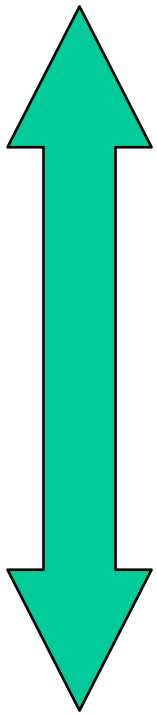
Alice

Eve

Bob

Message: HI BOB

01110100 10111001 00000101 10101001 01011100 01110100



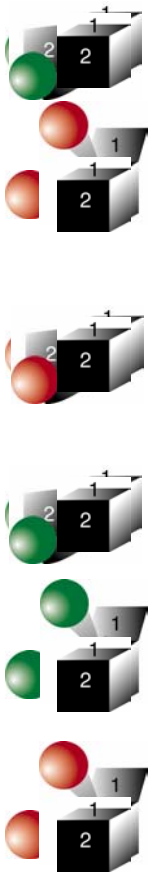
Alice and Bob can communicate privately if they share a random key that Eve doesn't know.

01110100 10111001 00000101 10101001 01011100 01110100

HI BOB

Alice

Bob

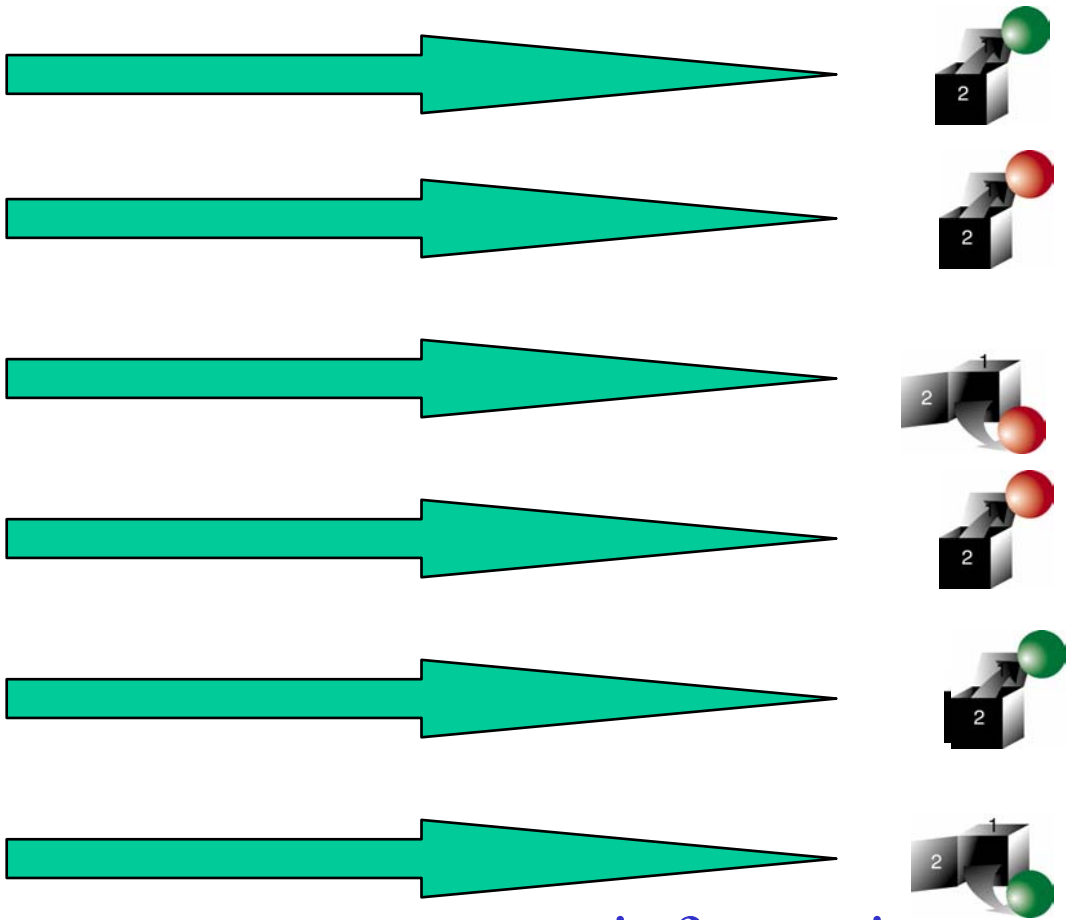


Alice can use quantum information (qubits) to send a random key to Bob.

Eve

Alice

Bob

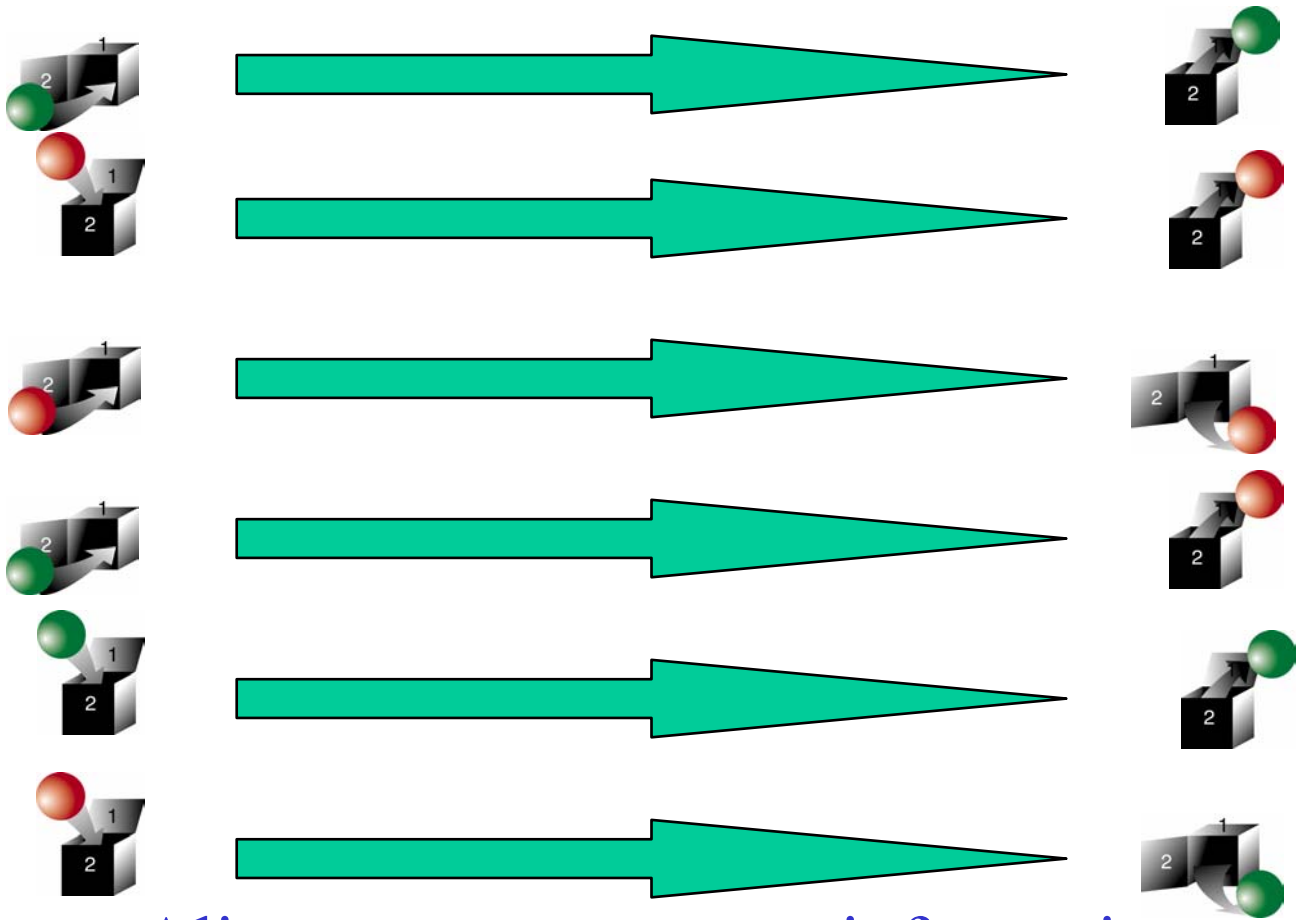


Alice can use quantum information (qubits) to send a random key to Bob.

Eve

Alice

Bob

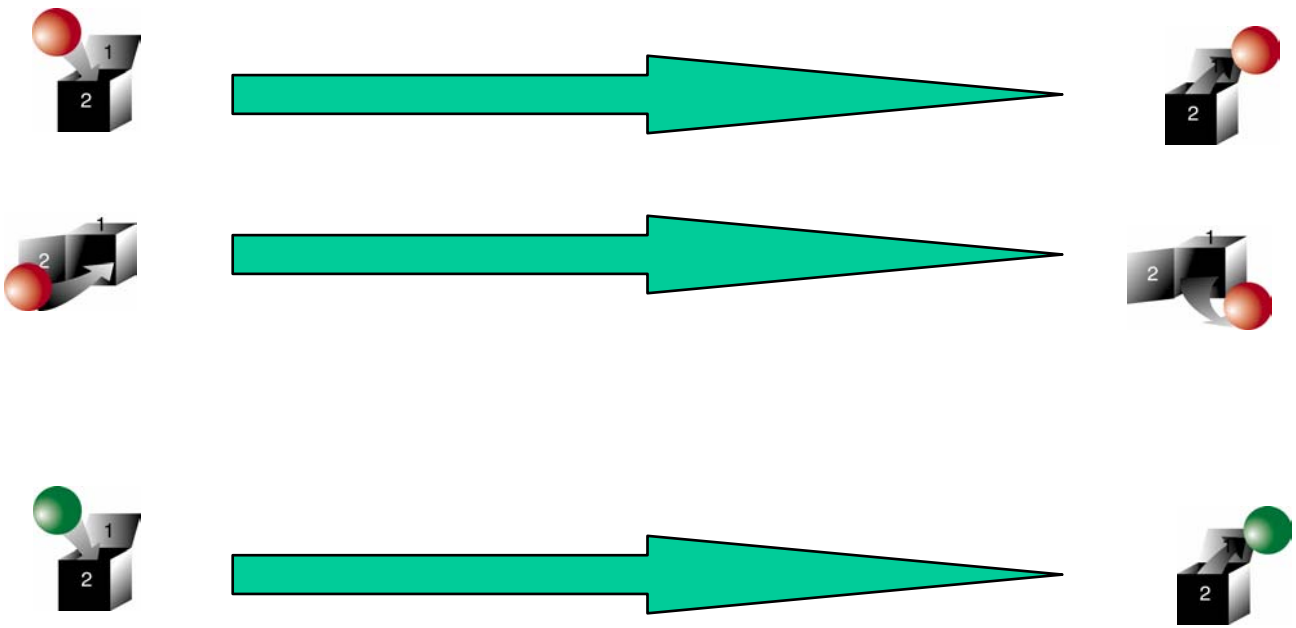


Alice can use quantum information (qubits) to send a random key to Bob.

Eve

Alice

Bob

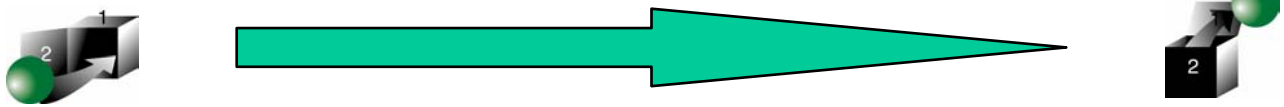


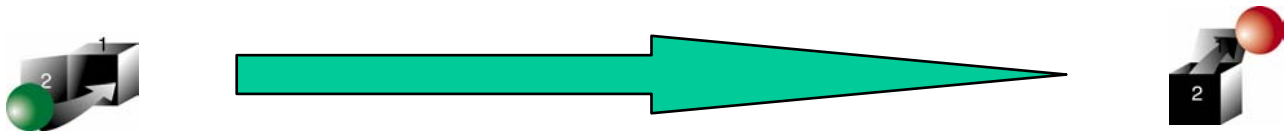
Alice can use quantum information (qubits) to send a random key to Bob.

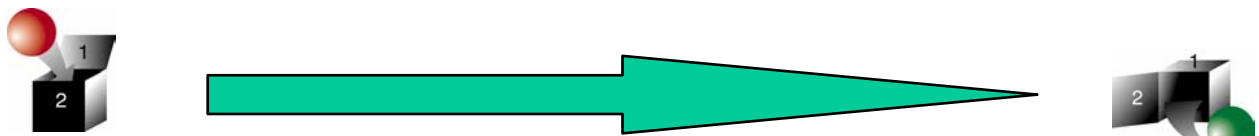
Eve

Alice

Bob







Alice can use quantum information (qubits) to send a random key to Bob.

Eve

Quantum News

"Spooky action at a distance"

January 15, 1997 Volume 1, Issue 1

Alice Announces Doors She Used!!

Alice

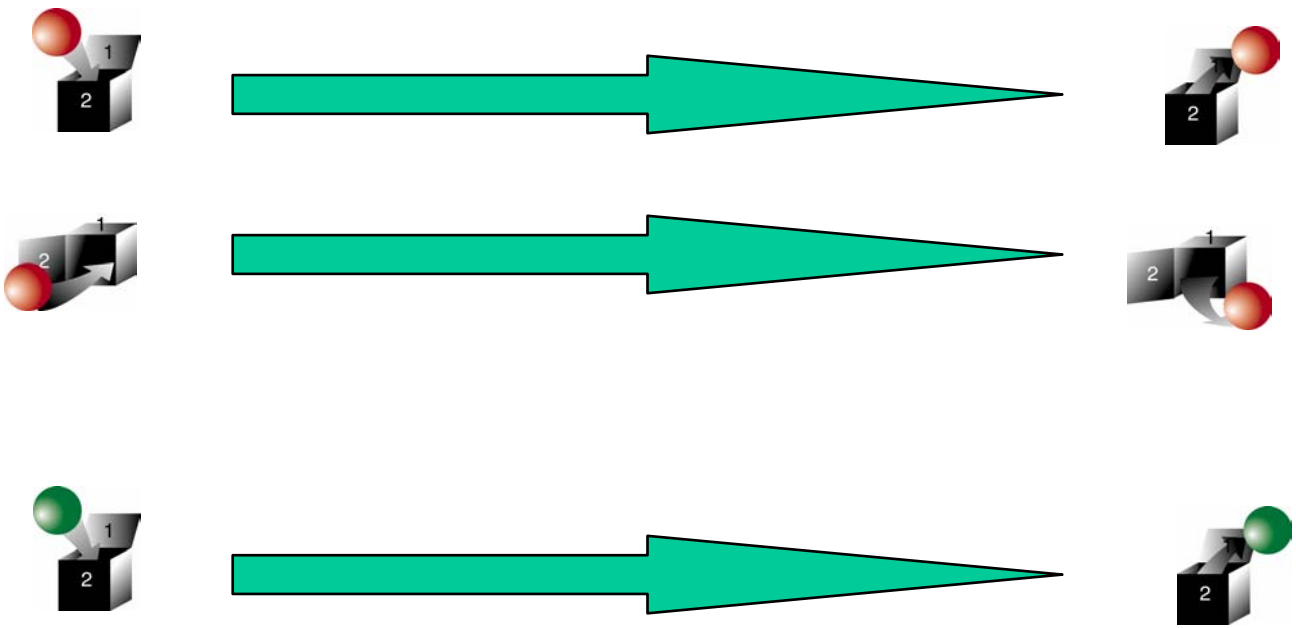
Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diem nonummy nibh euismod tincidunt ut lacreet dolore magna aliguam erat volutpat. Ut wisis enim ad minim veniam, quis nostrud exerci tution ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis te feugifacilisi. Duis autem dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit au gue duis dolore te feugat nulla facilisi. Ut wisi enim ad minim veniam, quis nostrud exerci taion ullamcorper suscipit lobortis nisl ut aliquip ex en commodo consequat. Duis te feugifacilisi.per suscipit lobortis nisl ut aliquip ex en commodo consequat. Duis te feugifacilisi. Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diem nonummy nibh euismod tincidunt ut lacreet dolore magna aliguam erat volutpat. Ut wisis enim ad minim veniam, quis nostrud exerci tution ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis te feugifacilisi. Duis autem dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit au gue duis dolore te feugat nulla facilisi.ipsum dolor sit amet, consectetuer adipiscing elit, sed diem nonummy nibh euismod tincidunt ut lacreet dolore magna aliguam erat volut-

Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diem nonummy nibh euismod tincidunt ut lacreet dolore magna aliguam erat volutpat. Ut wisis

Lorem Ipsum

Alice

Bob

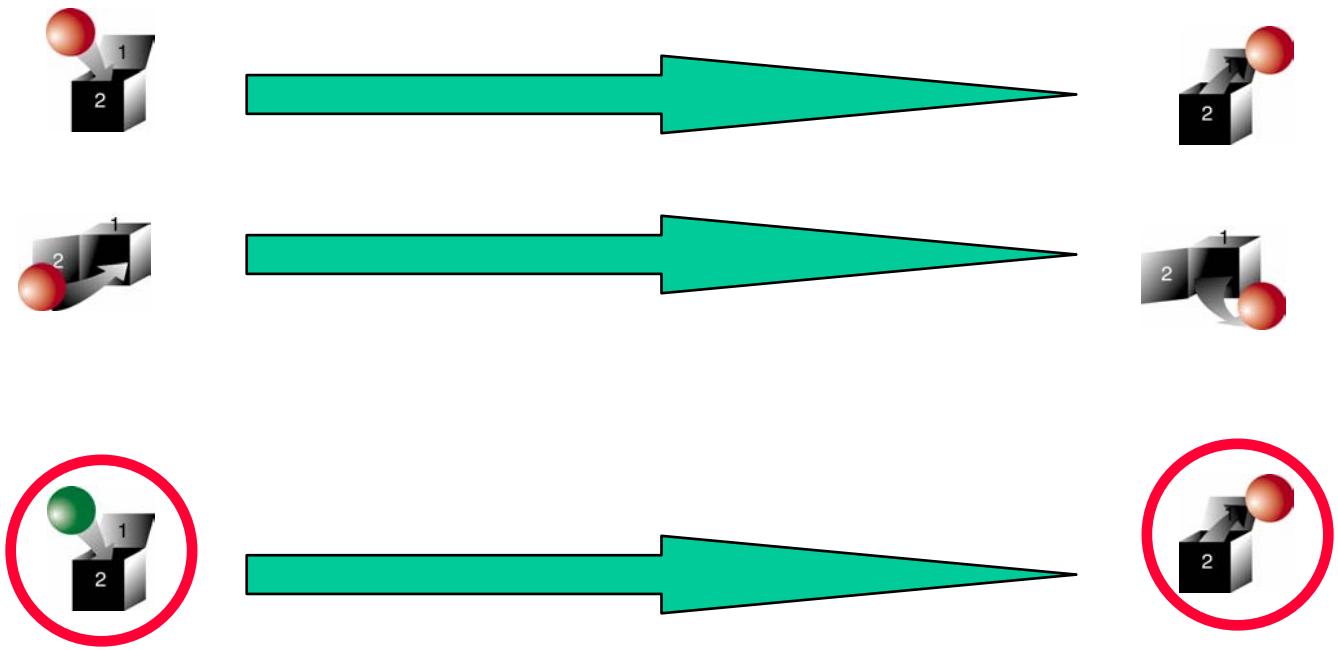


Alice can use quantum information (qubits) to send a random key to Bob.

Eve

Alice

Bob



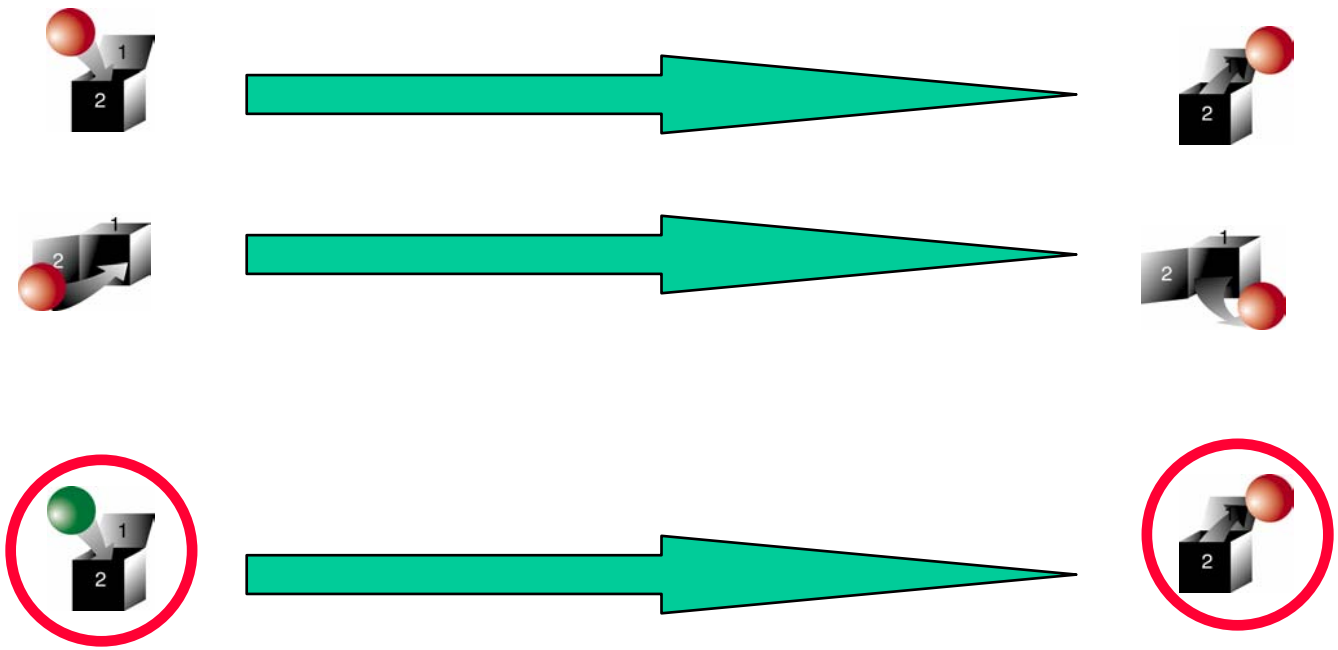
Alice can use quantum information (qubits) to send a random key to Bob.

Eve

Alice

Eve

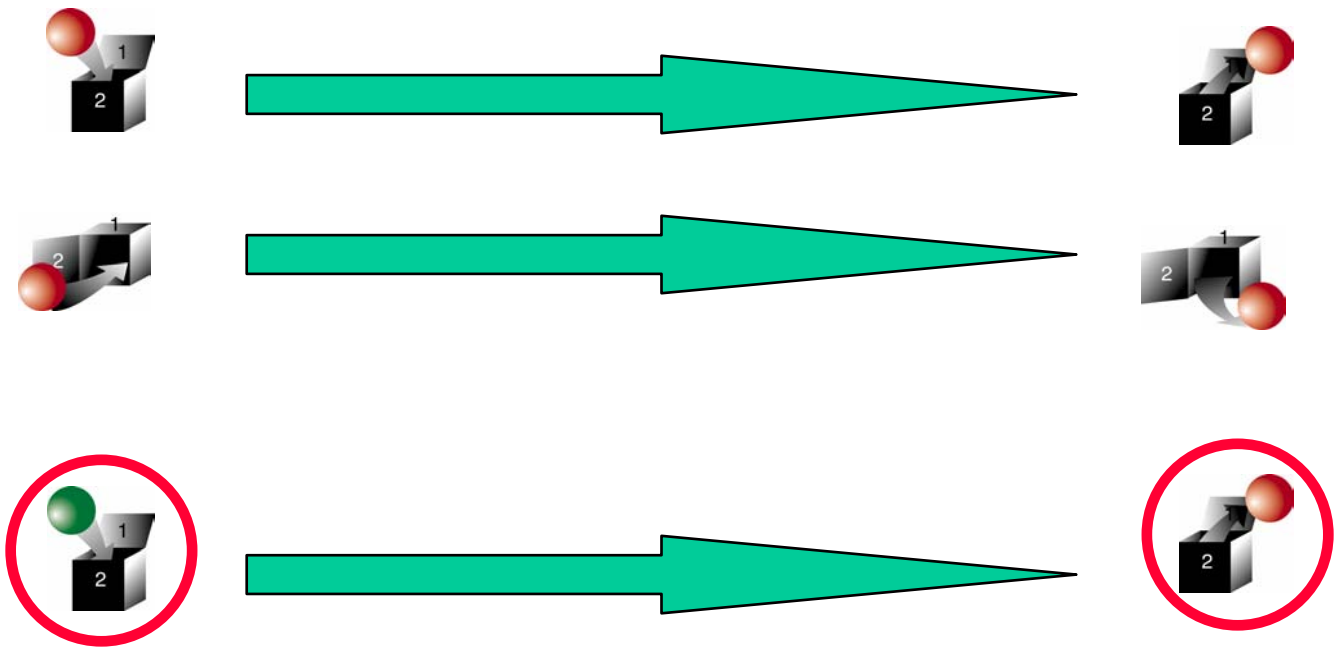
Bob



Alice can use quantum information (qubits) to send a random key to Bob.

Alice

Bob

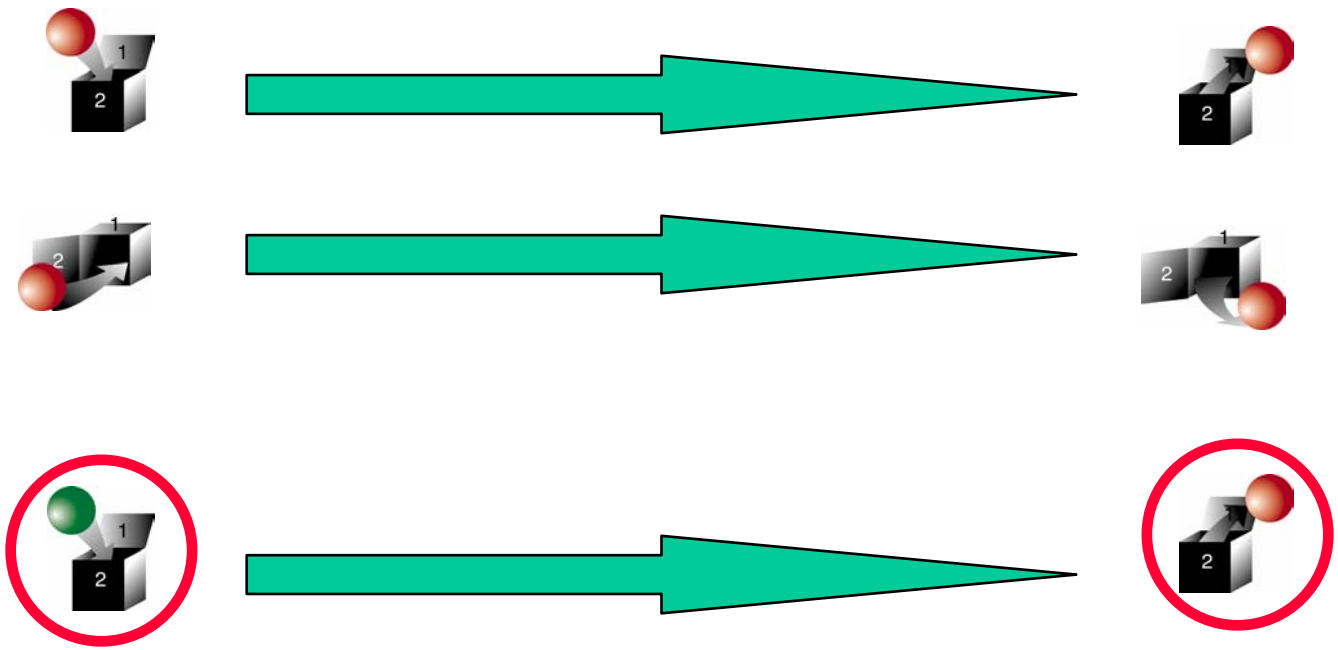


Alice can use quantum information (qubits) to send a random key to Bob.

Alice

Quantum key distribution, augmented by classical protocols that correct errors and amplify privacy, is *provably* secure against *arbitrary* eavesdropping attacks.

Bob



Alice can use quantum information (qubits) to send a random key to Bob.

Quantum Cryptography

Alice

Eve

Bob

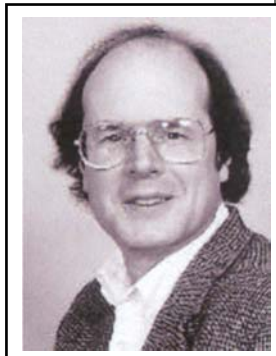
Privacy is founded on principles of fundamental physics, not the assumption that eavesdropping requires a difficult computation. Gathering information about a quantum state unavoidably disturbs the state.

QKD for sale!

Security is based on the principle that copying of quantum signals can be detected, a property not shared by classical information.

Experiments have demonstrated the feasibility of quantum key distribution (QKD) protocols in which single-photon pulses are sent through (150 km) telecom fibers.

Furthermore, quantum key distribution is now *commercially available*. You can order one over the (classical) Internet.

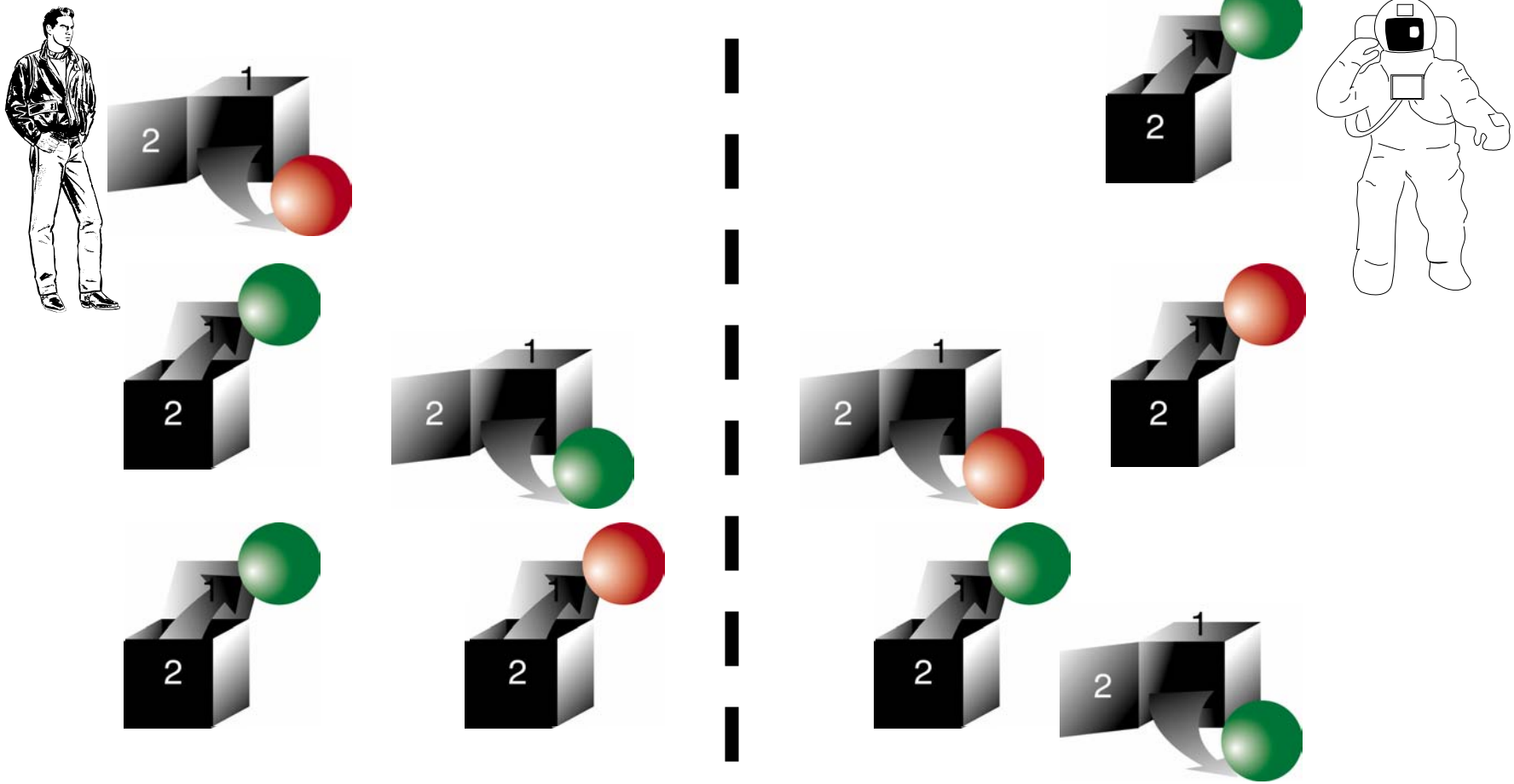


Bennett-Brassard ‘84

Quantum Correlations

Pasadena

Andromeda



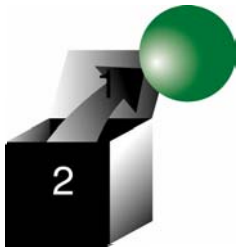
Open either door in Pasadena, and the color of the ball is *random*.

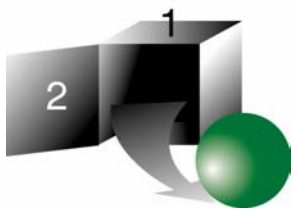
Same thing in Andromeda.

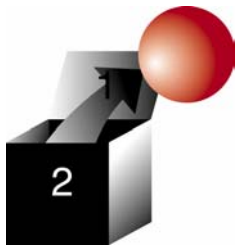
Quantum Correlations

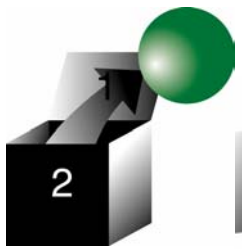
Pasadena

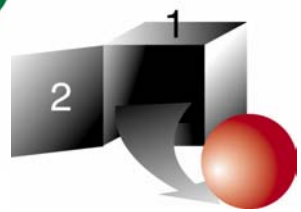
Andromeda

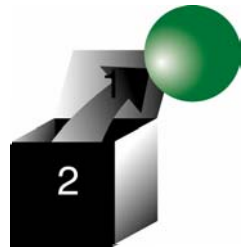


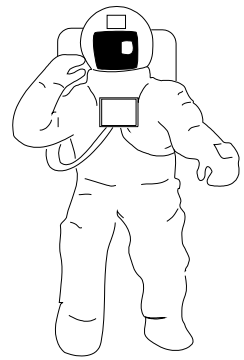


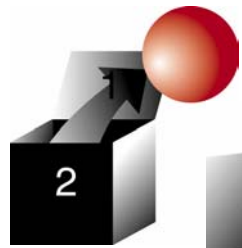


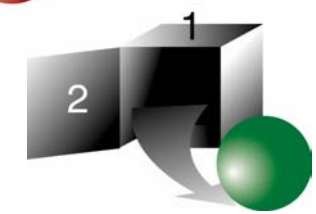


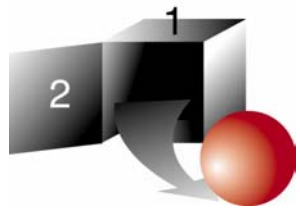


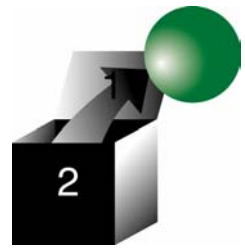










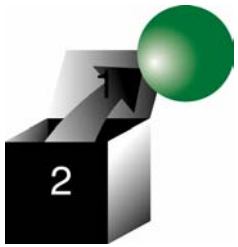


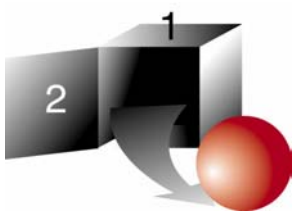
But if we both open the same door, we always find the same color.

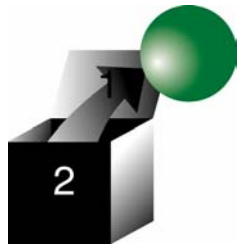
Quantum Correlations

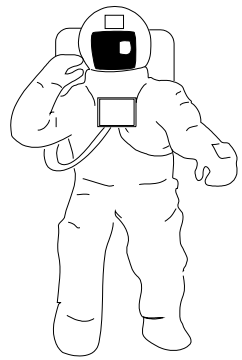
Pasadena

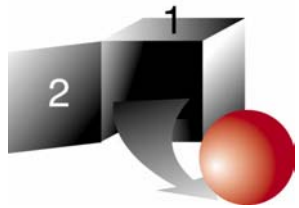
Andromeda





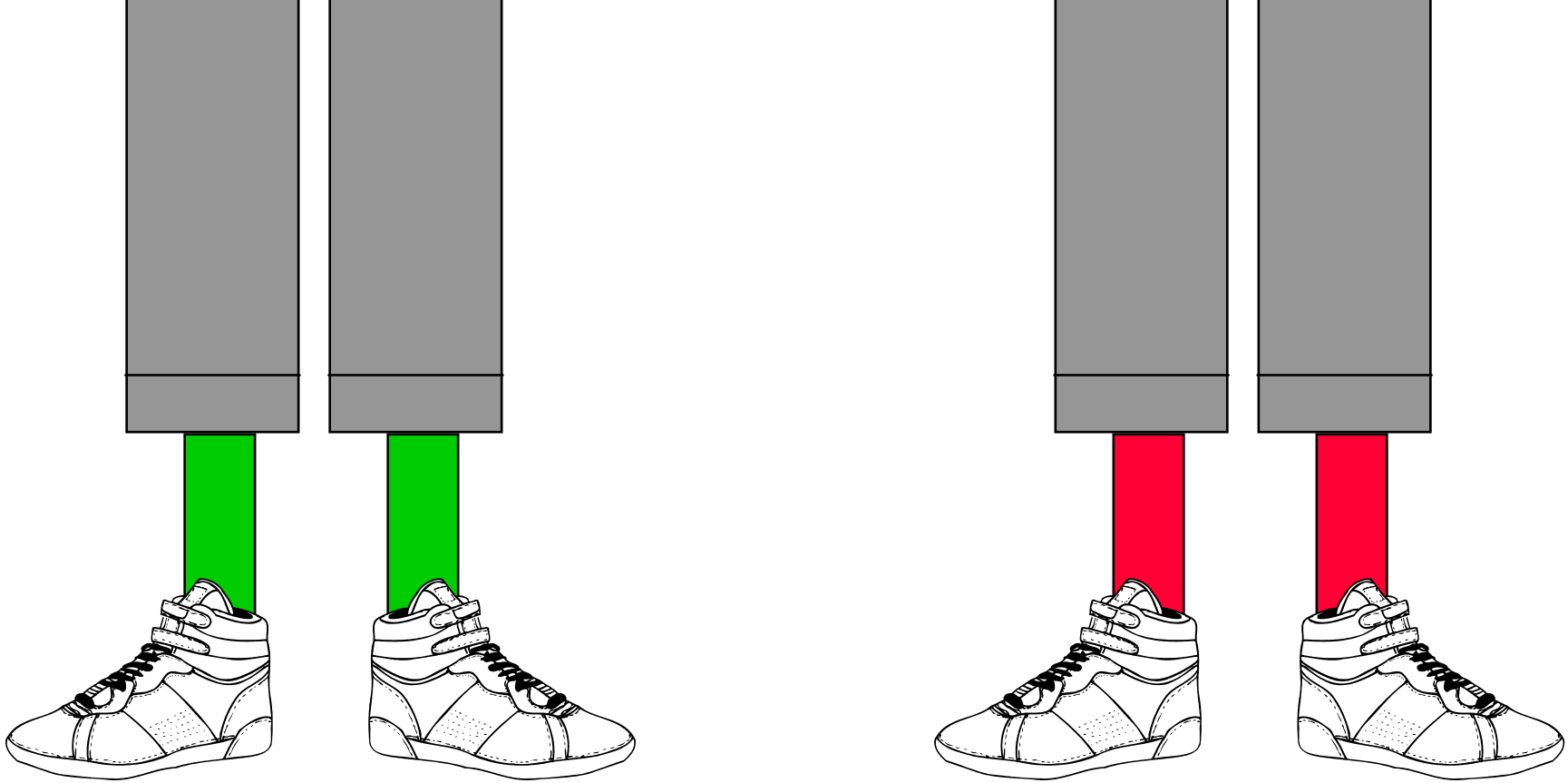




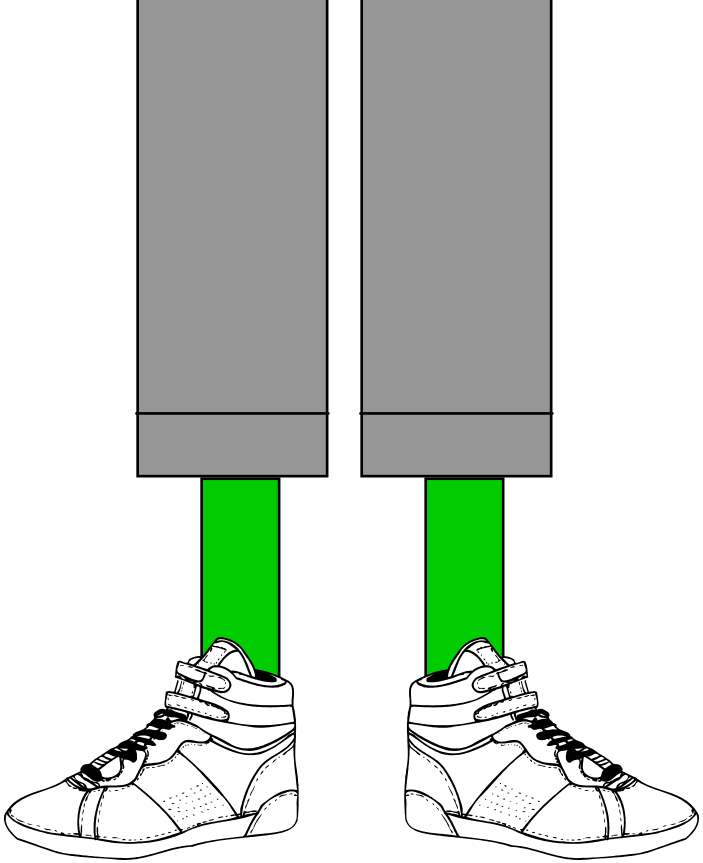


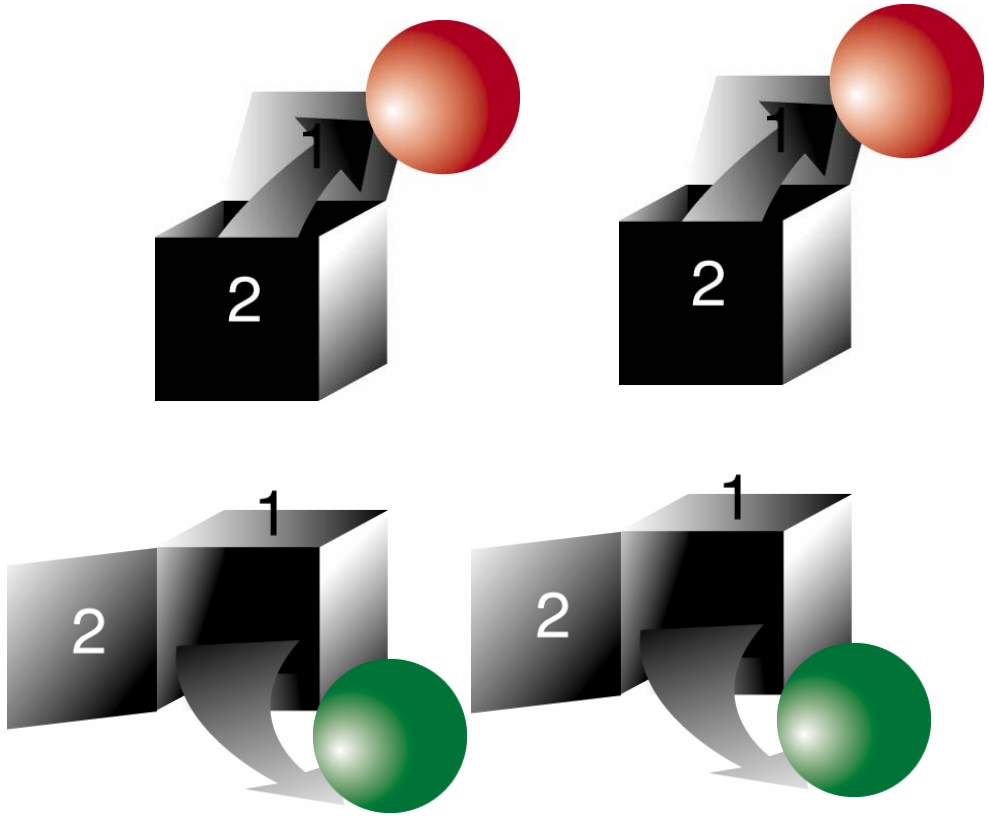
Quantum information can be *nonlocal*, shared equally by a box in Pasadena and a box in Andromeda.

This phenomenon, called *quantum entanglement*, is a crucial feature that distinguishes quantum information from classical information.



Classical Correlations





Classical Correlations

Quantum Correlations

Aren’t boxes like soxes?

MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

(Received March 25, 1935)

In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system. In quantum mechanics in the case of two physical quantities described by non-commuting operators, the knowledge of one precludes the knowledge of the other. Then either (1) the description of reality given by the wave function in quantum mechanics is not complete or (2) these two quantities cannot have simultaneous reality. Consideration of the problem of making predictions concerning a system on the basis of measurements made on another system that had previously interacted with it leads to the result that if (1) is false then (2) is also false. One is thus led to conclude that the description of reality as given by a wave function is not complete.

Einstein's 1935 paper, with Podolsky and Rosen (EPR), launched the theory of quantum entanglement. Arguably, it is the last paper of Einstein's career that still reverberates loudly today. To Einstein, quantum entanglement was so unsettling as to indicate that something is missing from our current understanding of the quantum description of Nature.

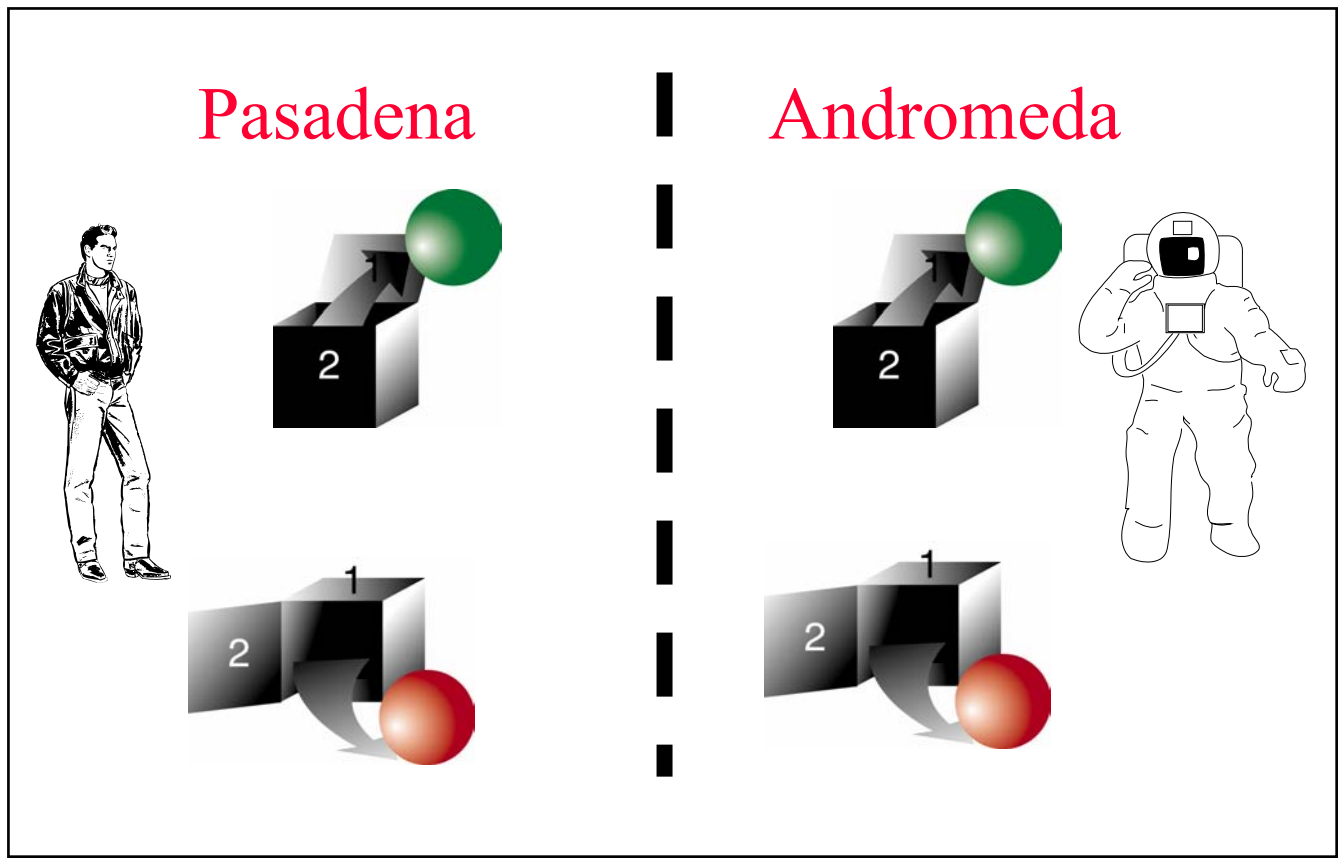
"Another way of expressing the peculiar situation is: the best possible knowledge of a *whole* does not necessarily include the best possible knowledge of its *parts* … I would not call that *one* but rather *the* characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought. By the interaction the two representatives [quantum states] have become entangled."

"It is rather discomforting that the theory should allow a system to be steered or piloted into one or the other type of state at the experimenter's mercy in spite of his having no access to it."

Erwin Schrödinger, *Proceedings of the Cambridge Philosophical Society*, submitted 14 August 1935

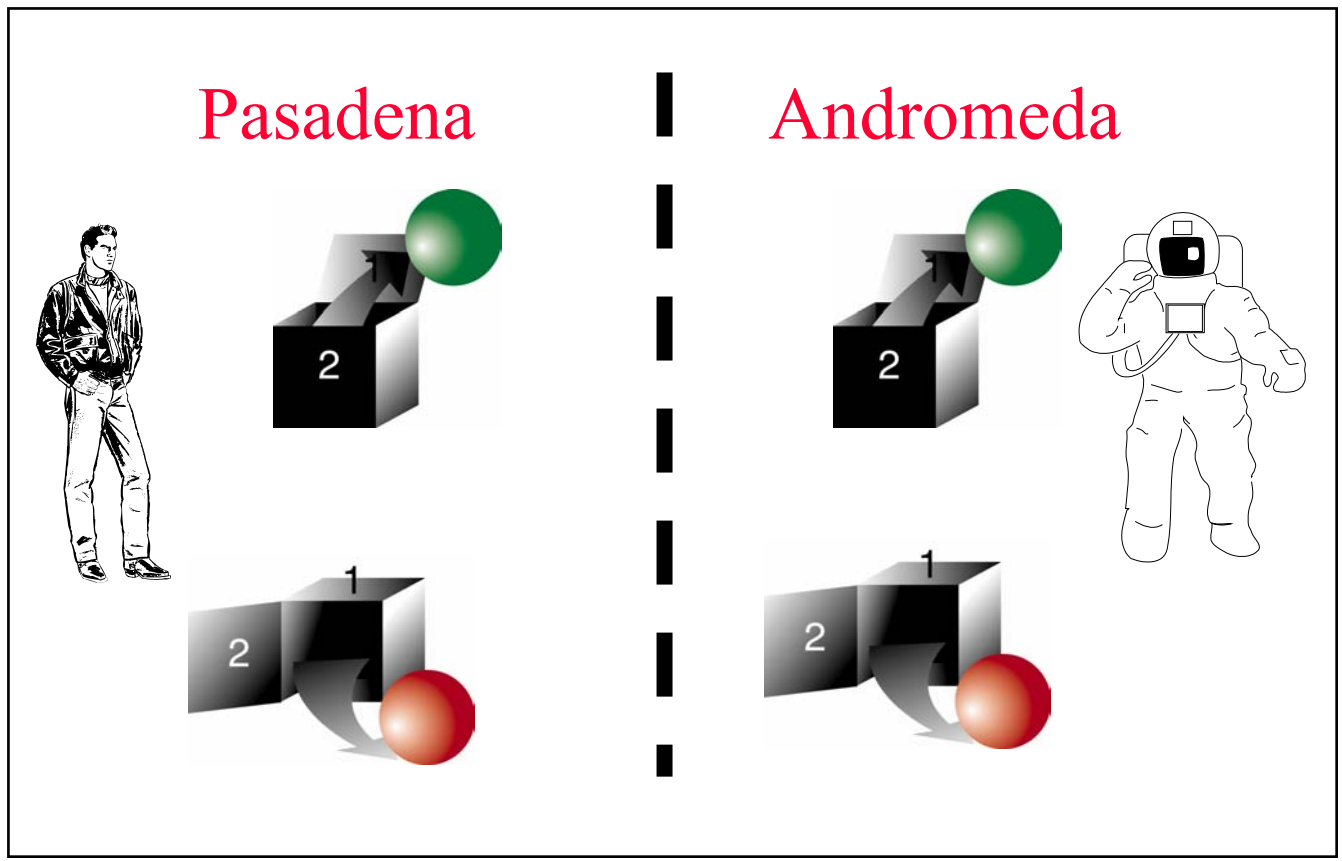
Quantum Entanglement

Bell ‘64



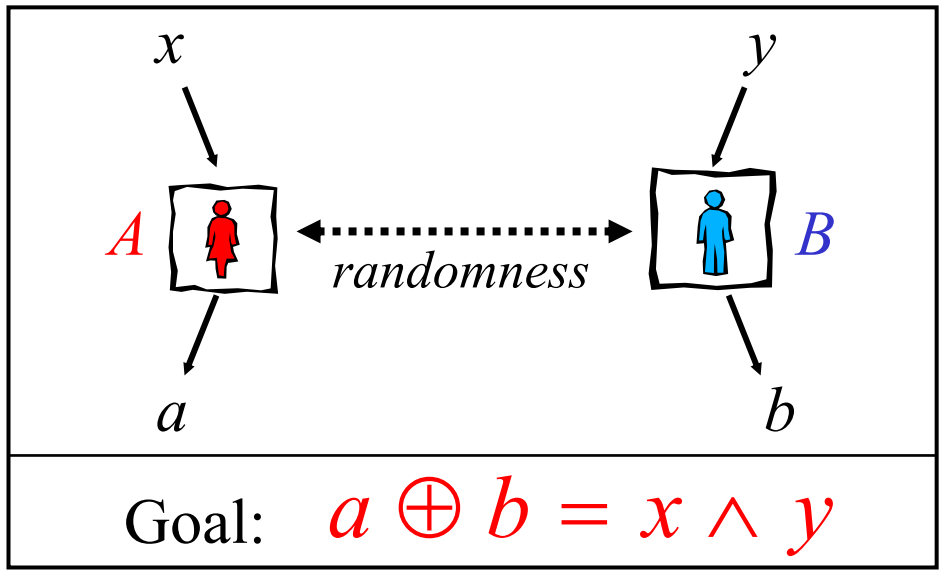
Quantum information can be *nonlocal*; quantum correlations are a stronger resource than classical correlations.

Bell ‘64



Quantum entanglement

Alice and Bob are cooperating, but distantly separated, players on the same team, playing a game. They cannot communicate, but in order to win the game, they must make correlated moves.

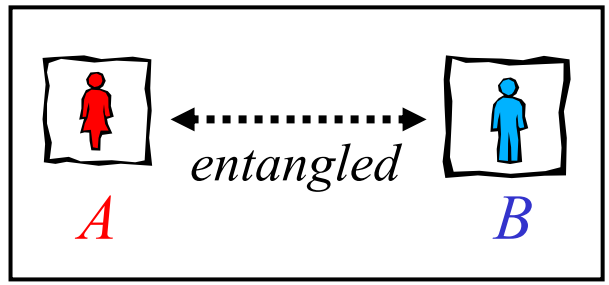


Bell's theorem (1964): If Alice and Bob share classically correlated bits (which were prepared before the game began), they can win the game with probability no higher than 75% (averaged over all possible inputs), but if they share quantumly correlated qubits (quantum entanglement), they can win the game with probability 85.4%.

This example illustrates that *quantum correlations are a stronger resource than classical correlations*, enabling us to perform tasks that would otherwise be impossible.

Quantum entanglement

Bell's theorem (1964): Alice and Bob have a higher probability of winning the game if they share quantumly correlated qubits (quantum entanglement) than if they shared classically correlated bits.



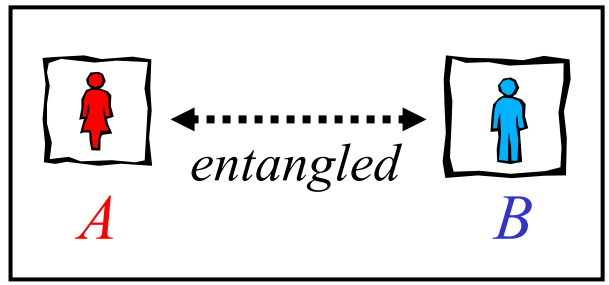
In experimental tests, physicists have played the game (e.g. with entangled photons – Aspect, 1982) and have won with a probability that exceeds what is possible classically (though there are still loopholes to these tests!).

Quantum information can be *nonlocal*; quantum correlations are a stronger resource than classical correlations.

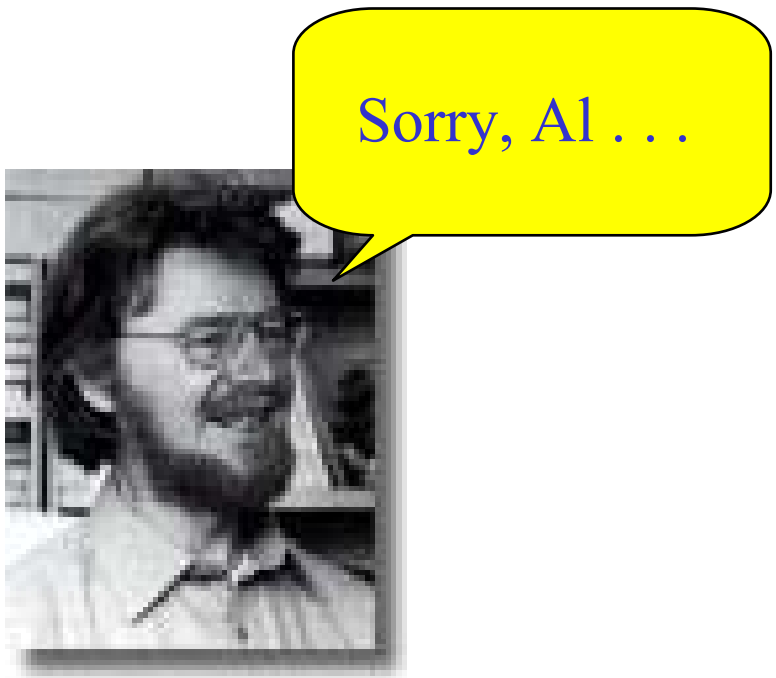
* Spooky action at a distance!!

Quantum entanglement

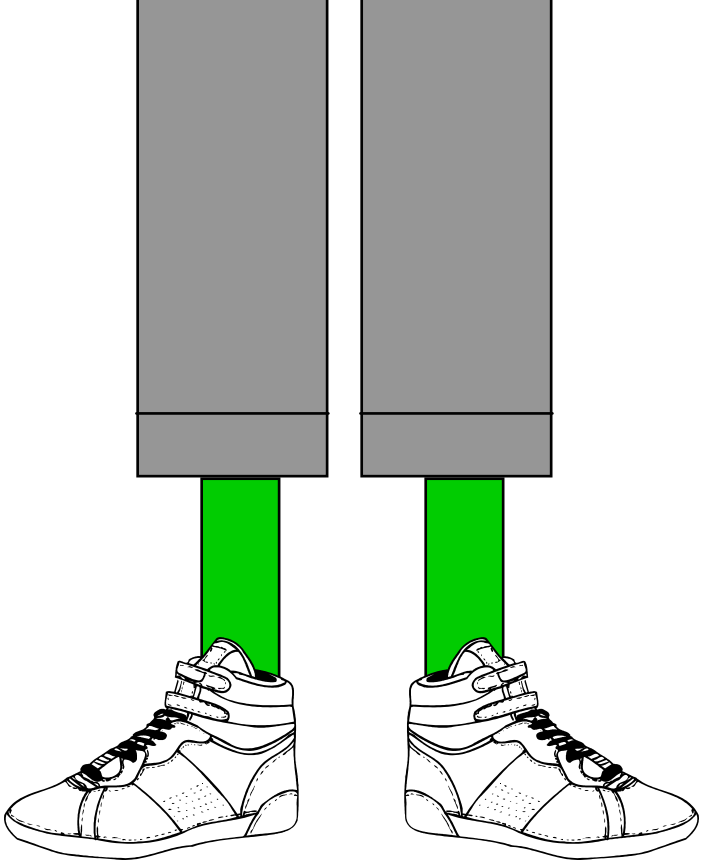
Bell's theorem (1964): Alice and Bob have a higher probability of winning the game if they share quantumly correlated qubits (quantum entanglement) than if they shared classically correlated bits.

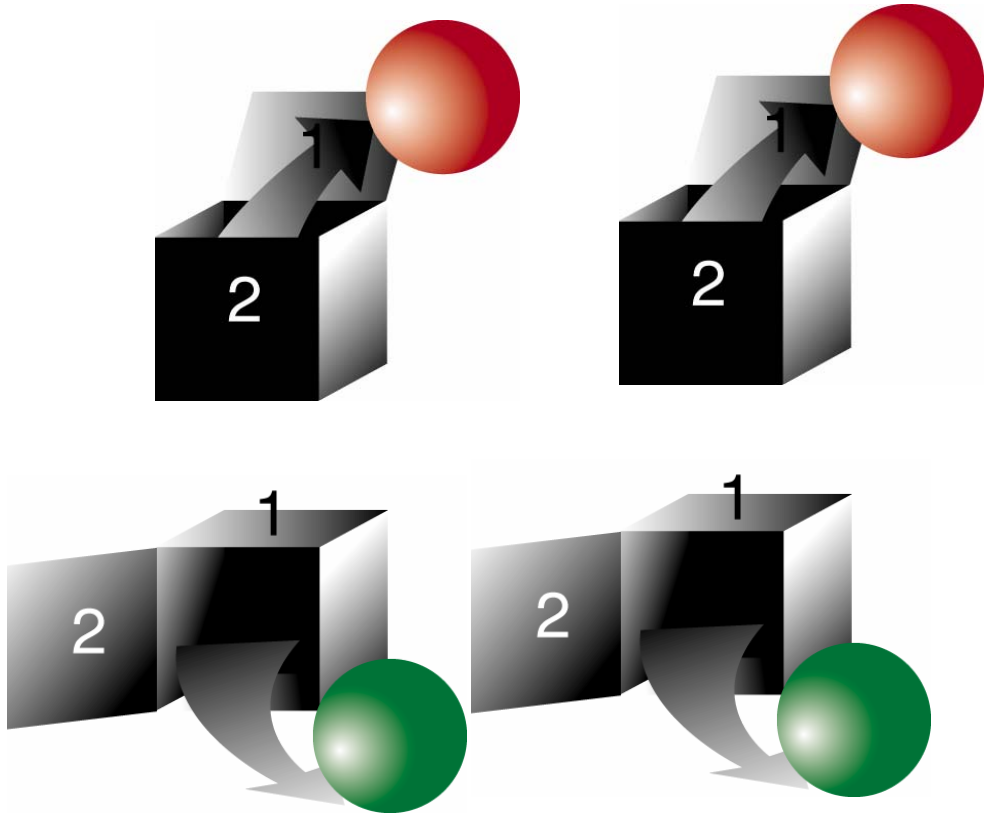


In experimental tests, physicists have played the game (e.g. with entangled photons – Aspect, 1982) and have won with a probability that exceeds what is possible classically (though there are still loopholes to these tests!).



* Spooky action at a distance!!

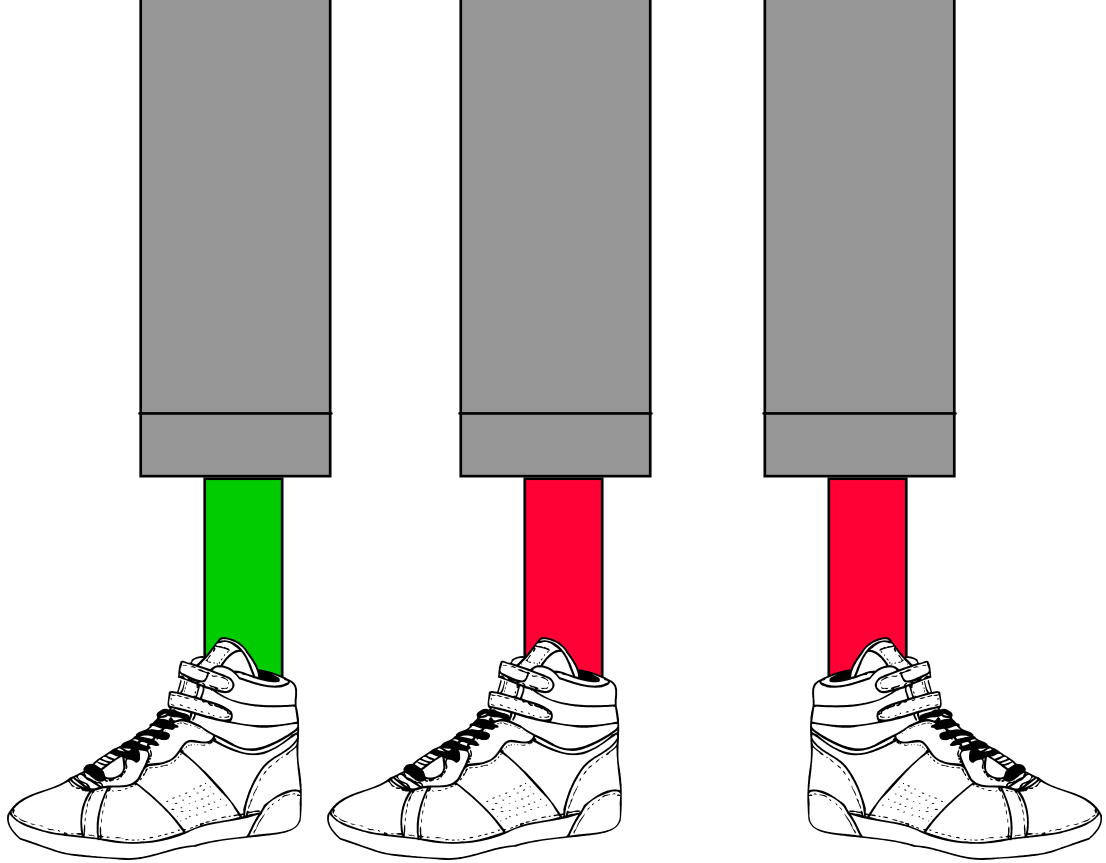




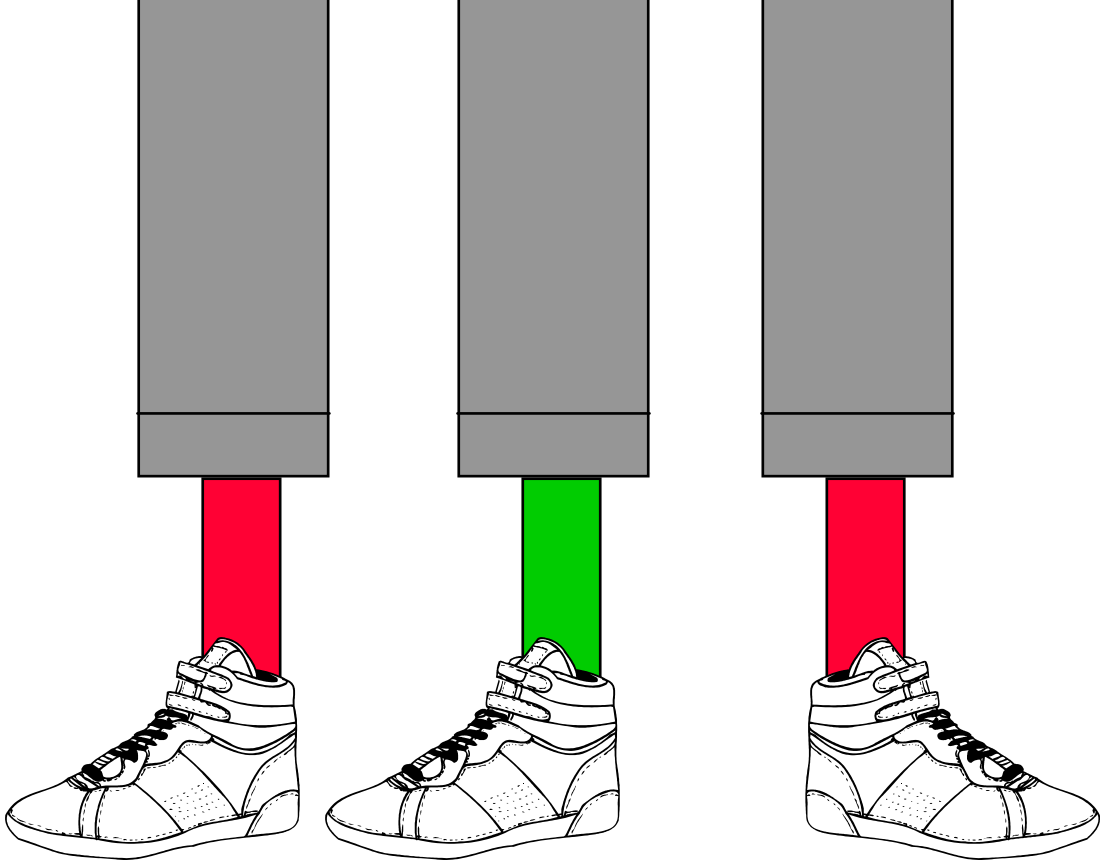
Classical Correlations

Quantum Correlations

Aren’t boxes like soxes?

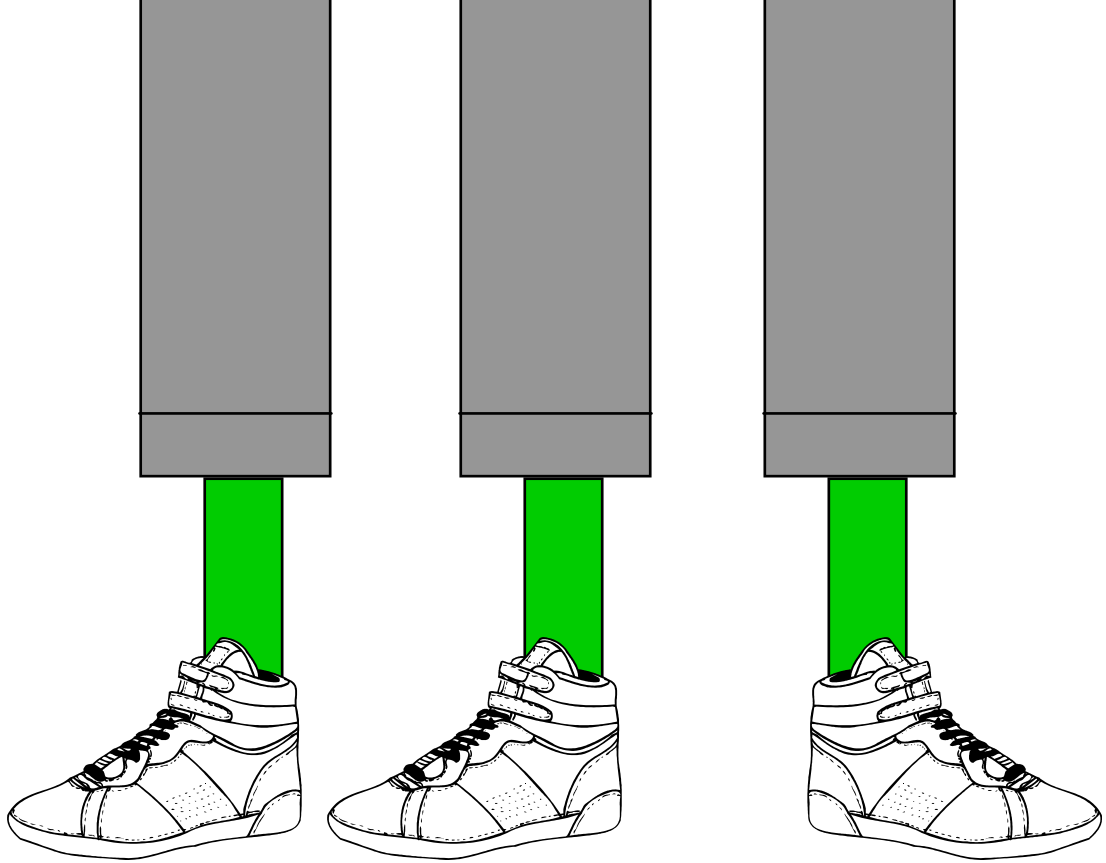


Always: an even number of red socks.
an odd number of green socks.



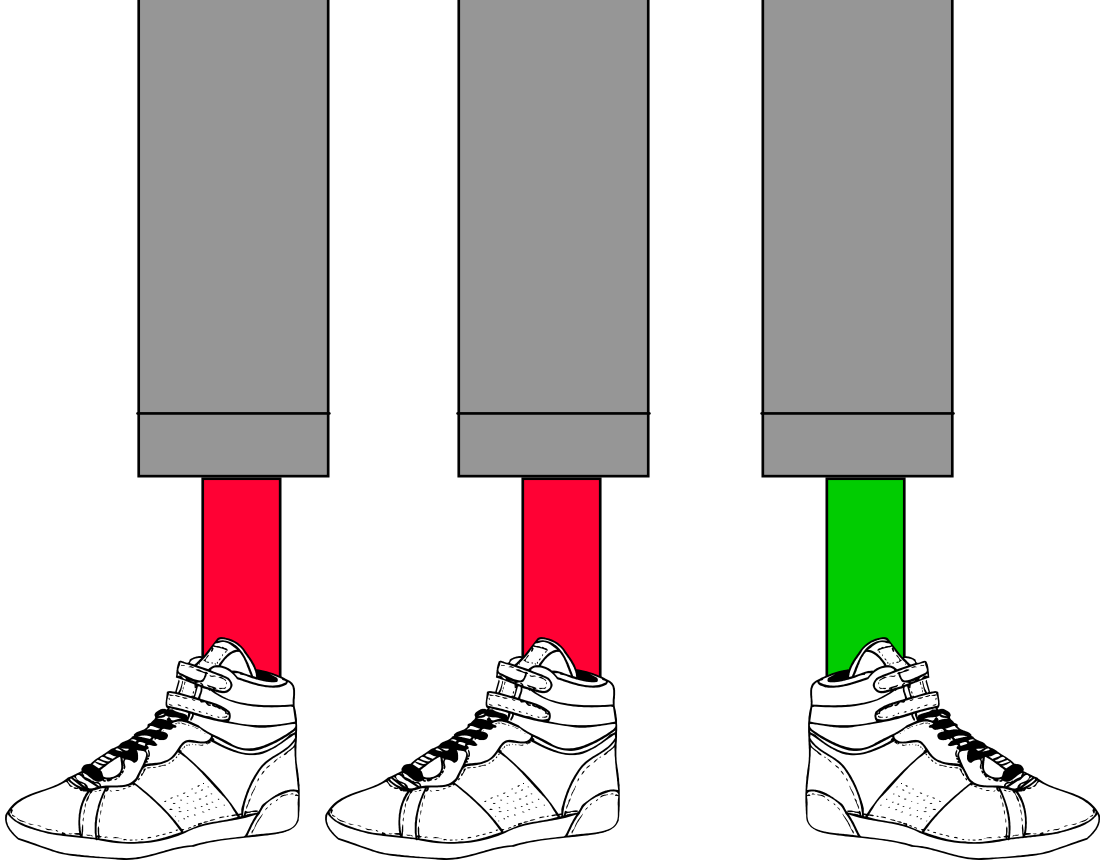
Always: an even number of red socks.

an odd number of green socks.



Always: an even number of red socks.

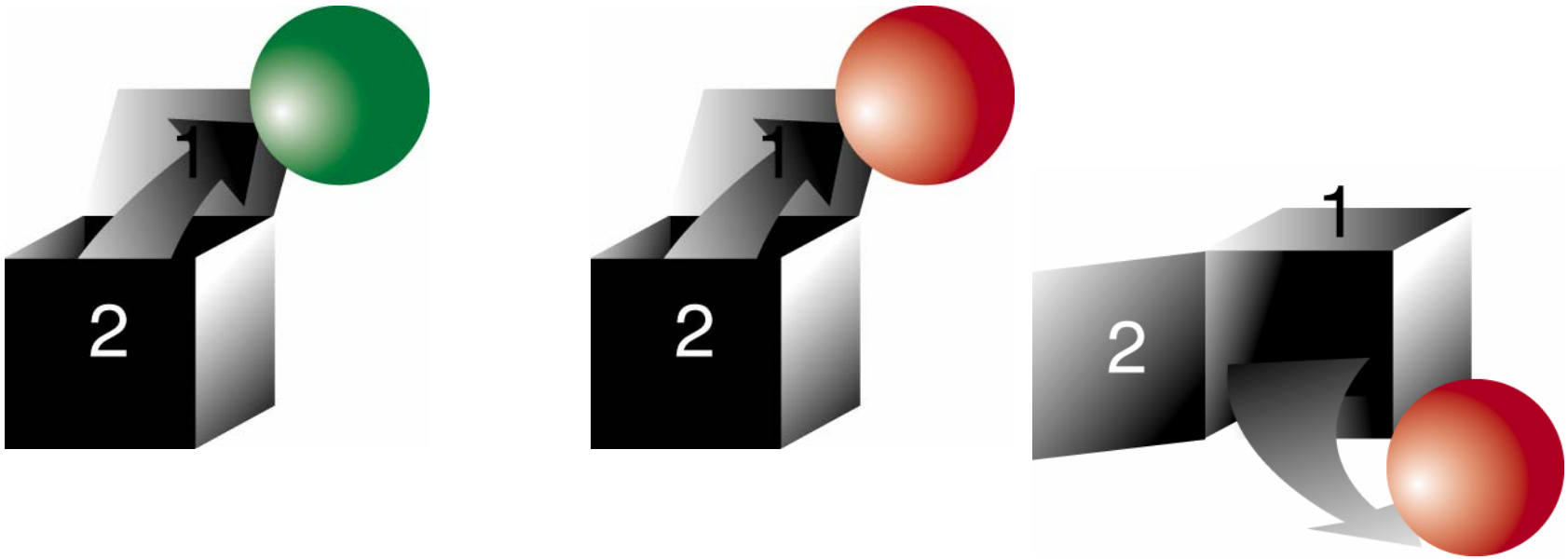
an odd number of green socks.



Always: an even number of red socks.

an odd number of green socks.

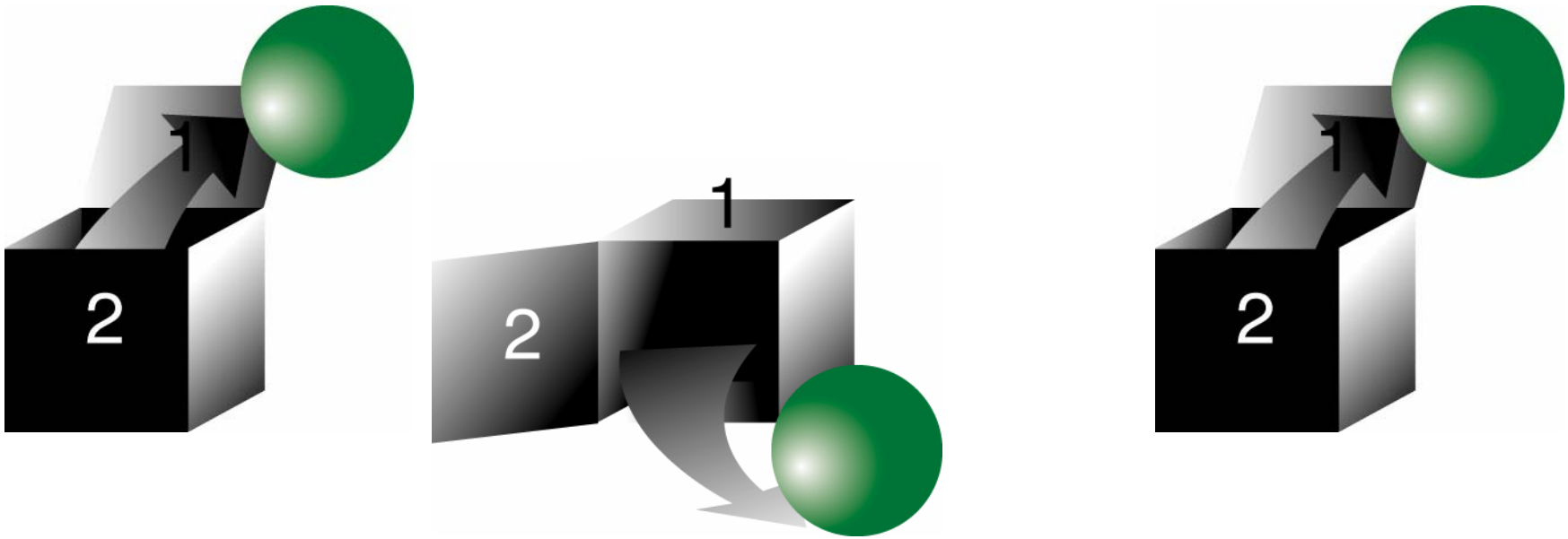
Pasadena Chicago New York



We open door number 1 of two of the boxes, and open door number 2 of the other box.

We *always* find an even number of red balls and an odd number of green balls.

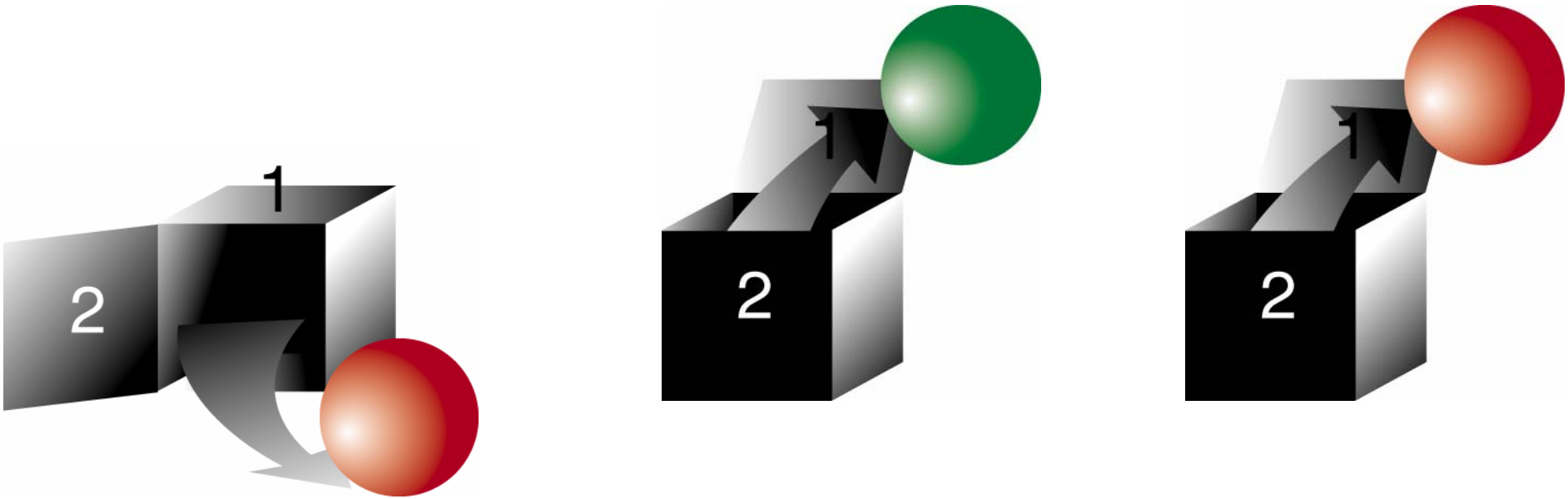
Pasadena Chicago New York



We open door number 1 of two of the boxes, and open door number 2 of the other box.

We *always* find an even number of red balls and an odd number of green balls.

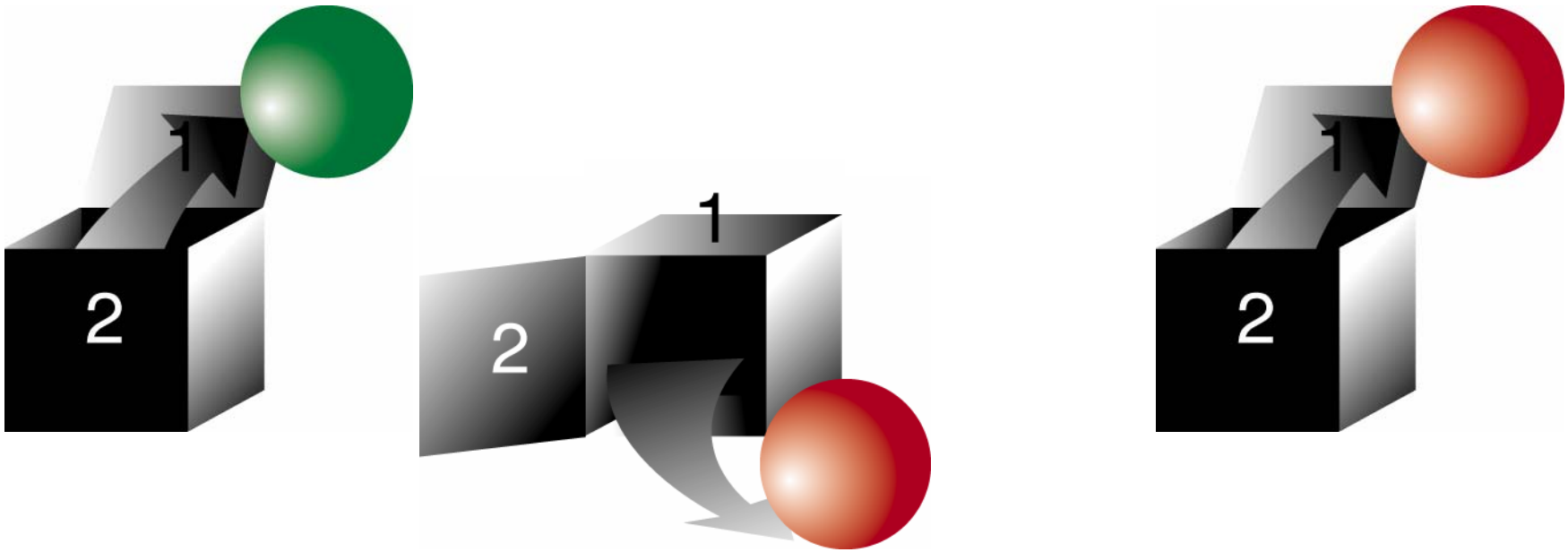
Pasadena Chicago New York



We open door number 1 of two of the boxes, and open door number 2 of the other box.

We *always* find an even number of red balls and an odd number of green balls.

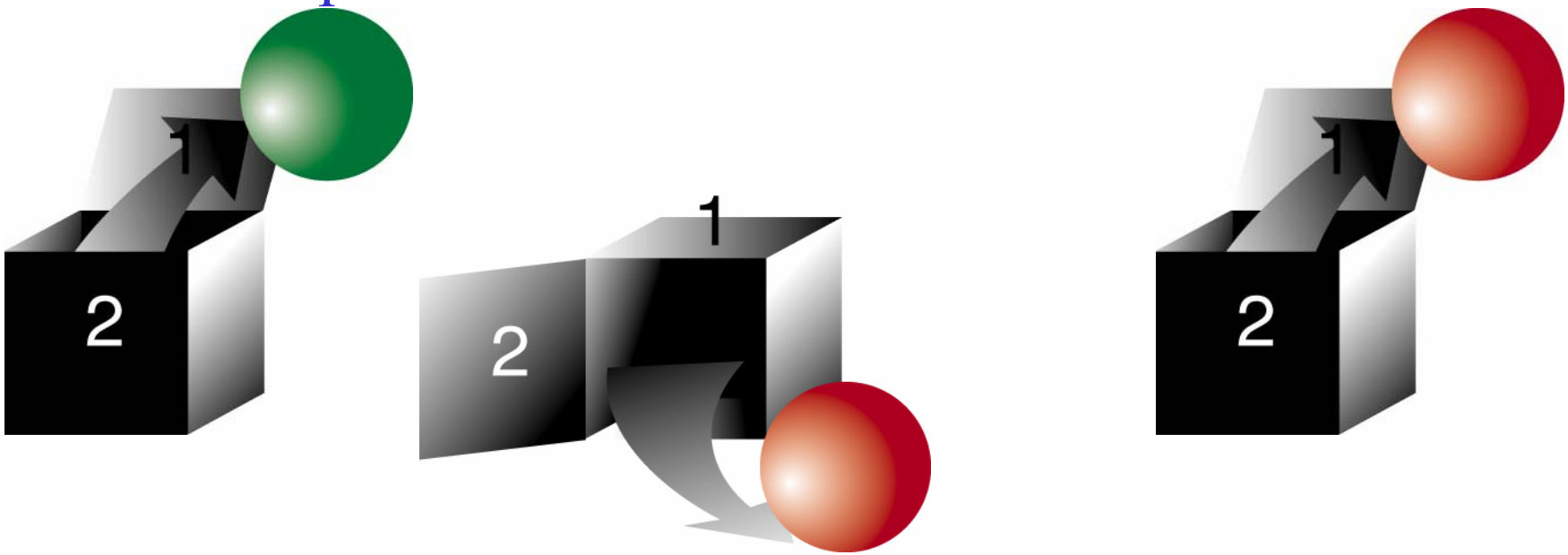
Pasadena Chicago New York



We open door number 1 of two of the boxes, and open door number 2 of the other box.

We *always* find an even number of red balls and an odd number of green balls.

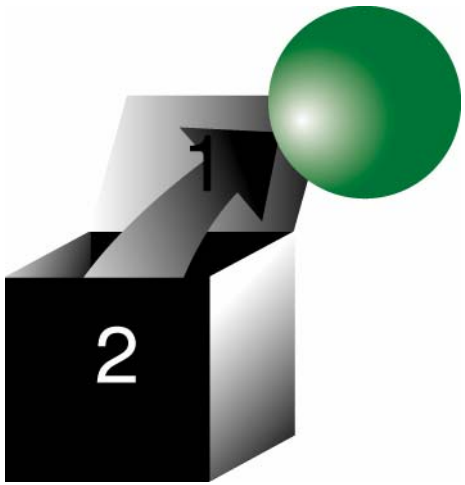
We open door number 1 of two of the boxes,
and open door number 2 of the other box.

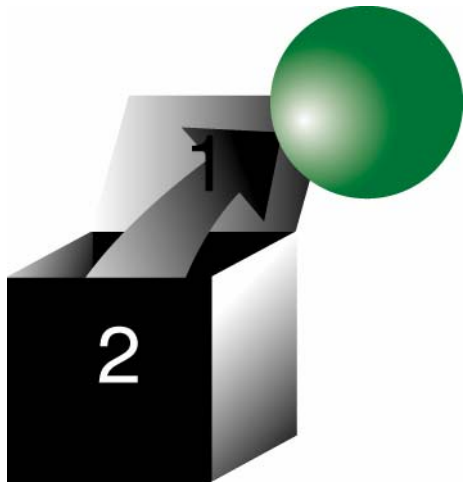


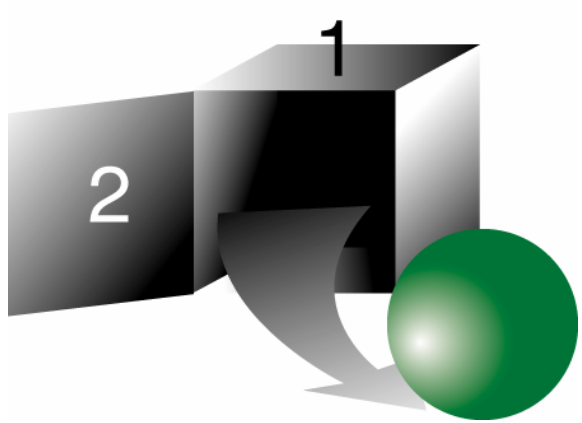
We *always* find an even number of red
balls and an odd number of green balls.

By opening doors of the first two boxes,
we can determine what will happen if we
open *either* door 1 or door 2 in the third box.

We open door number 1 of two of the boxes,
and open door number 2 of the other box.



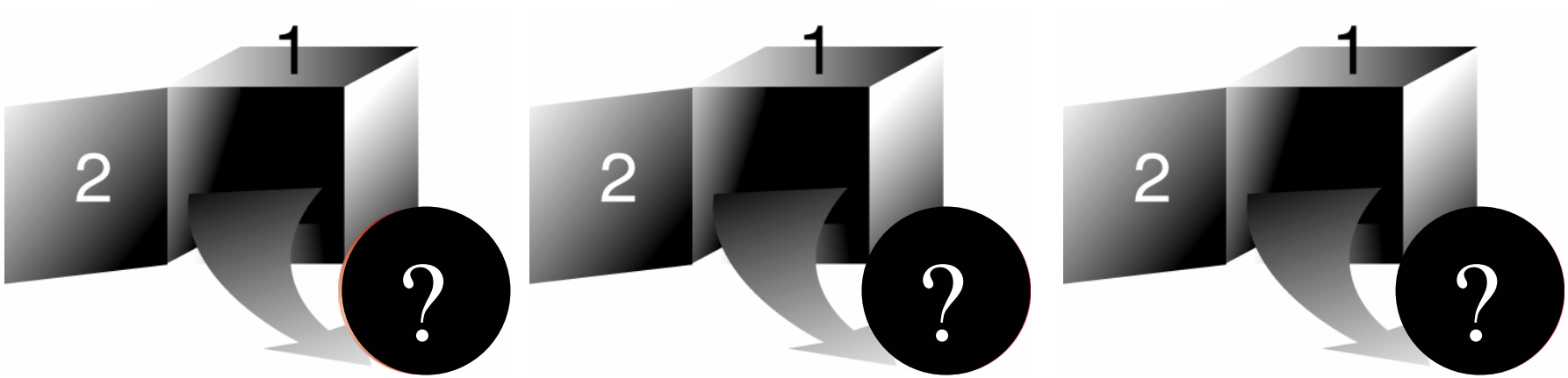




We *always* find an even number of red
balls and an odd number of green balls.

By opening doors of the first two boxes,
we can determine what will happen if we
open *either* door 1 or door 2 in the third box.

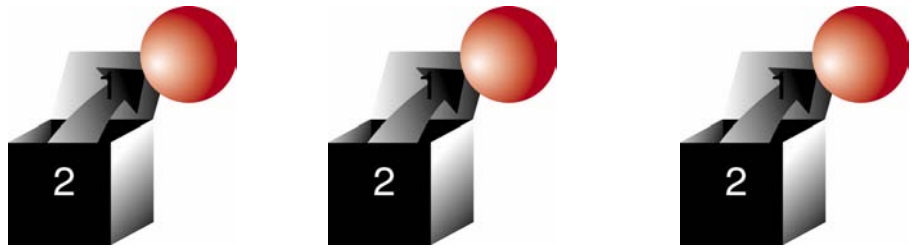
If we open door number 1 of two boxes, and open door number 2 of the other box, we *always* find an even number of red balls and an odd number of green balls.



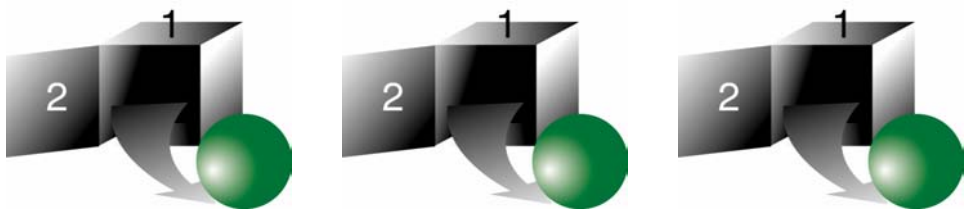
But . . . what will happen if we open door number 2 of all three boxes?

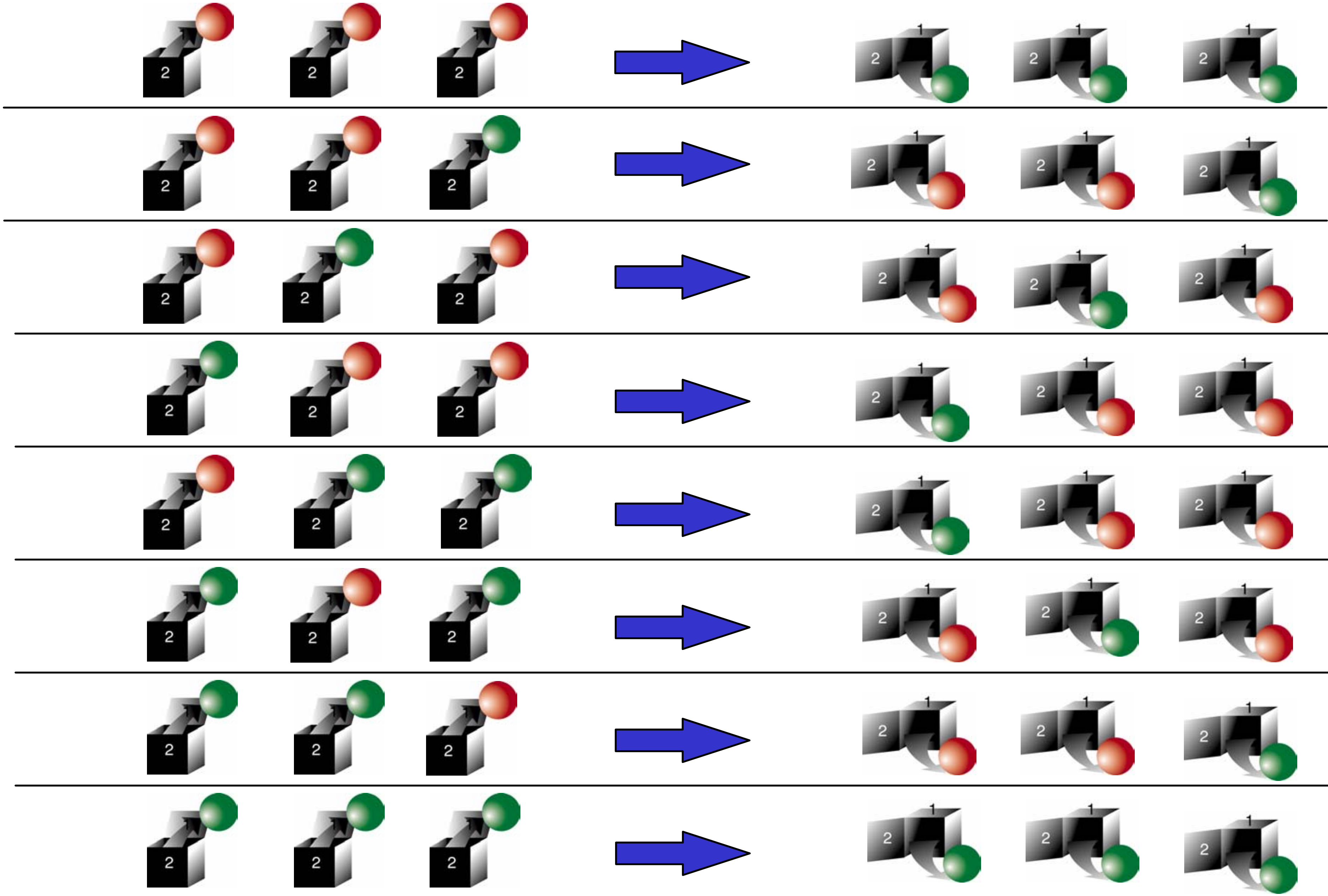
If we open door number 1 of two boxes, and open door number 2 of the other box, we *always* find an even number of red balls and an odd number of green balls.

If . . .

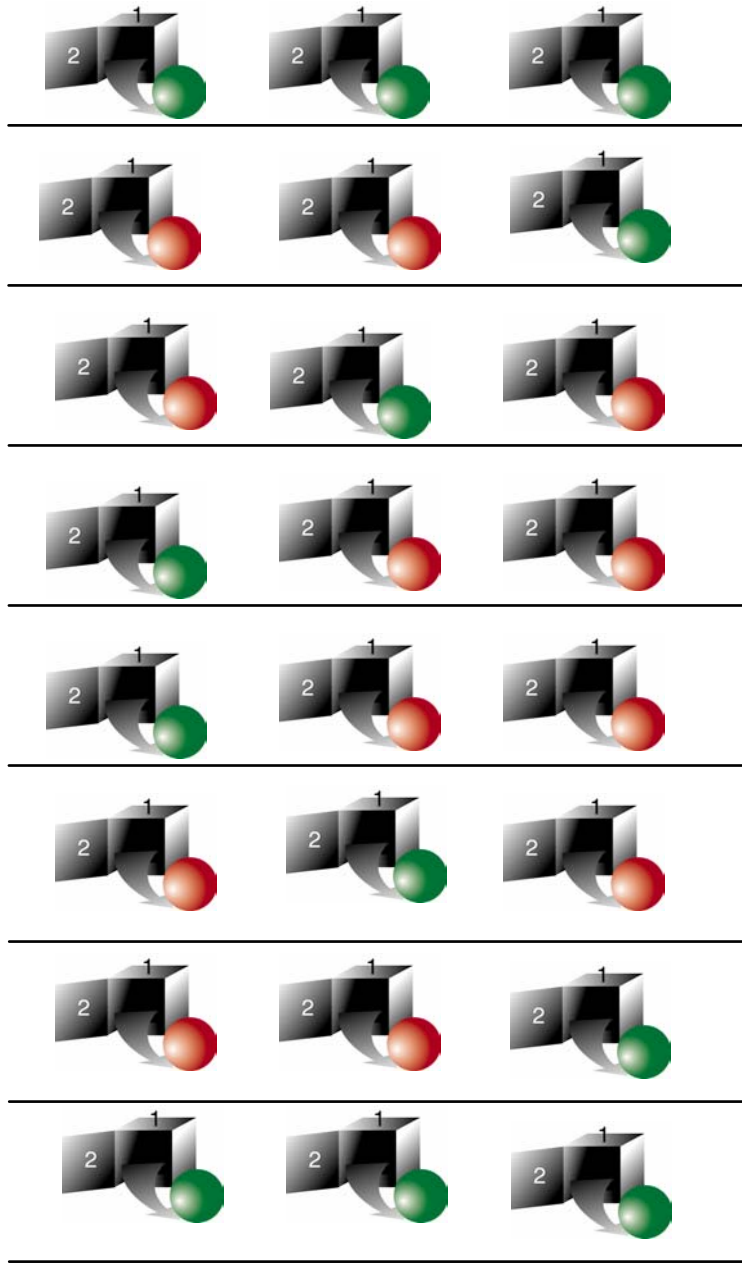


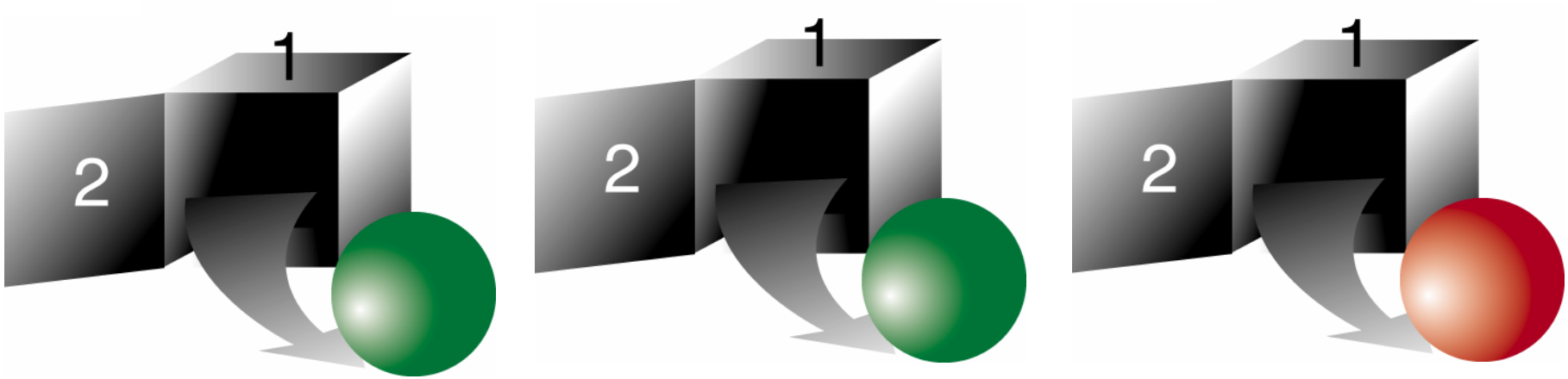
then . . .



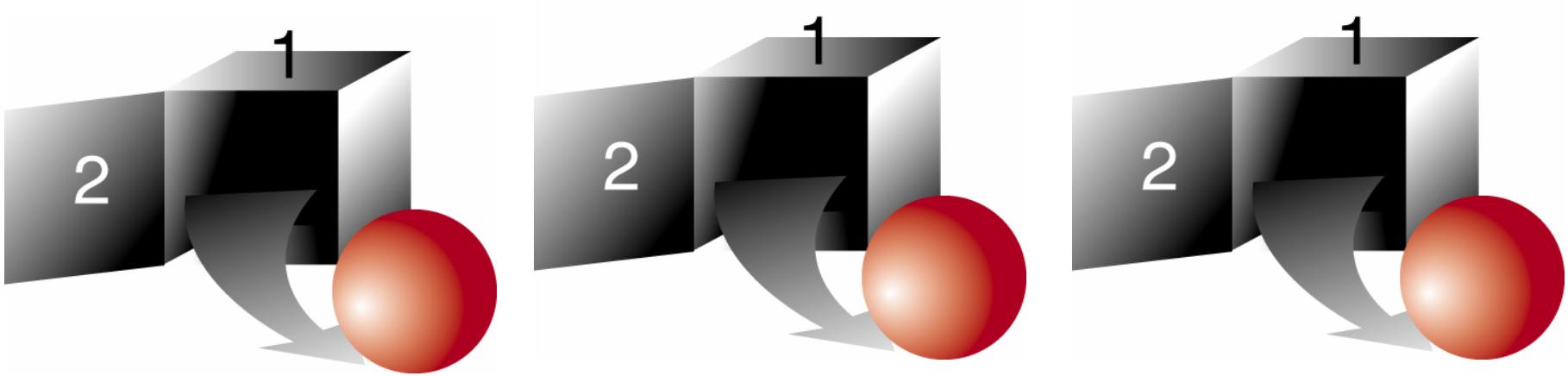


If we open door number 2 of all three boxes, we expect that the number of red balls will always be even, and the number of green balls will always be odd.

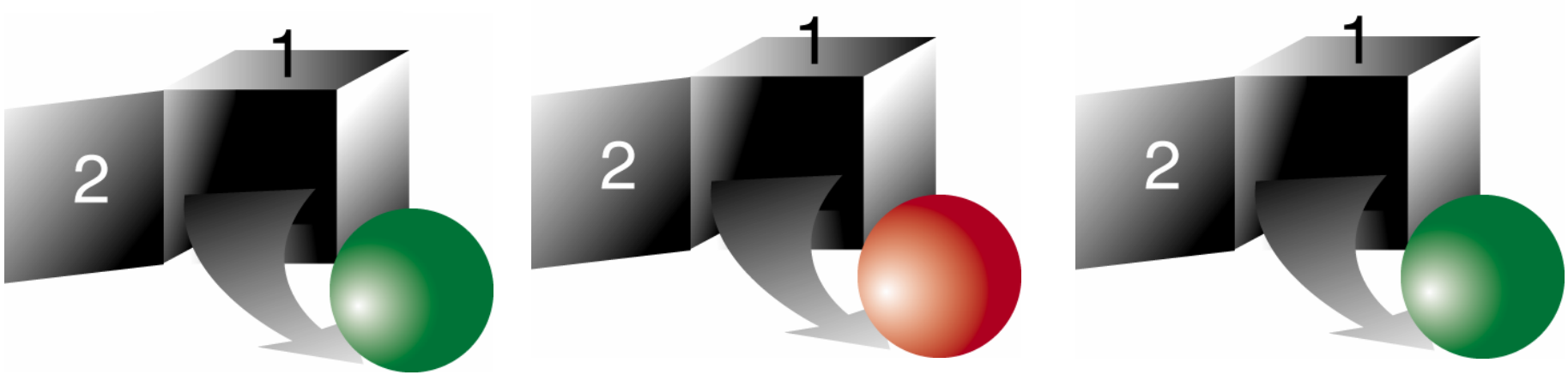




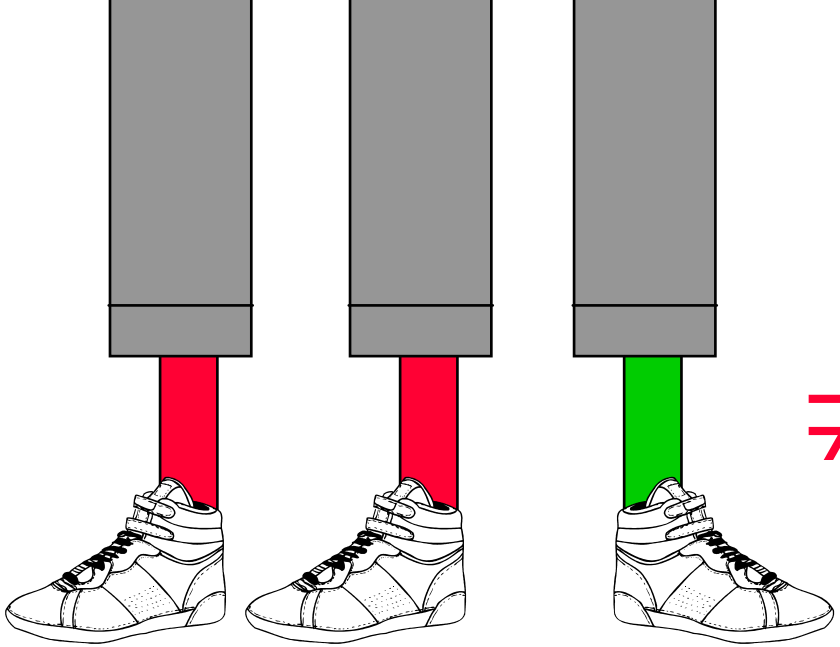
But, in fact, when we open door number 2 on all three boxes, we find an odd number of red balls and an even number of green balls!



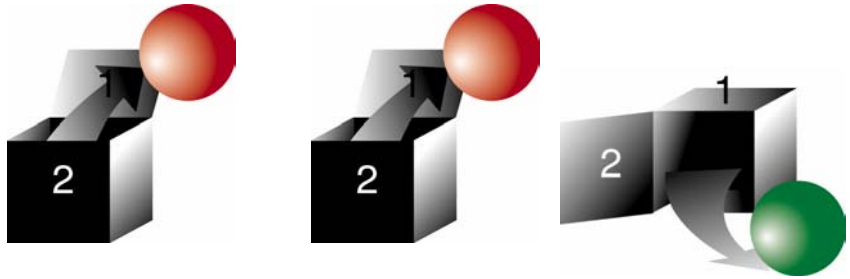
But, in fact, when we open door number 2 on all three boxes, we find an odd number of red balls and an even number of green balls!



But, in fact, when we open door number 2 on all three boxes, we *always* find an odd number of red balls and an even number of green balls!



≠



Boxes are *not* like soxes!

When the three quantum boxes are entangled, opening two of the boxes seems to "*influence*" what will happen when we open the third box! (But in a subtle way that does not allow us to send a message from one box to another.)

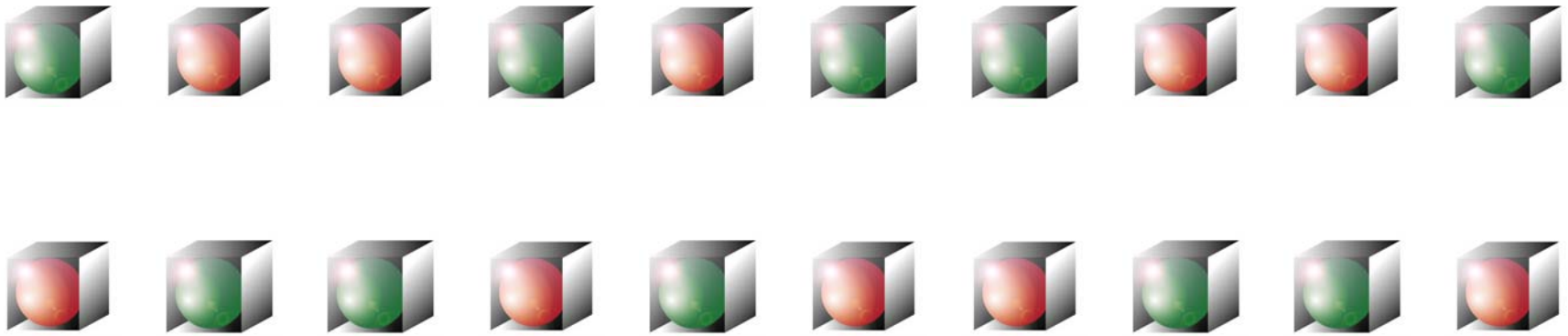
We must not reason based on what might have happened but did not in fact happen (e.g., "what if we had opened door number 1 instead of door number 2?").

10 classical bits.

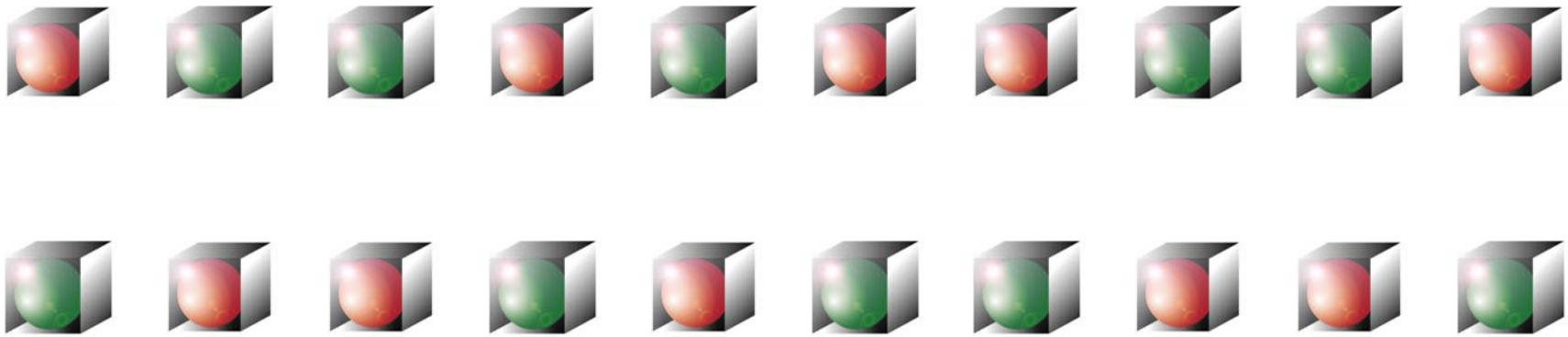
10 classical bits.

1,000 numbers to describe 10 qubits

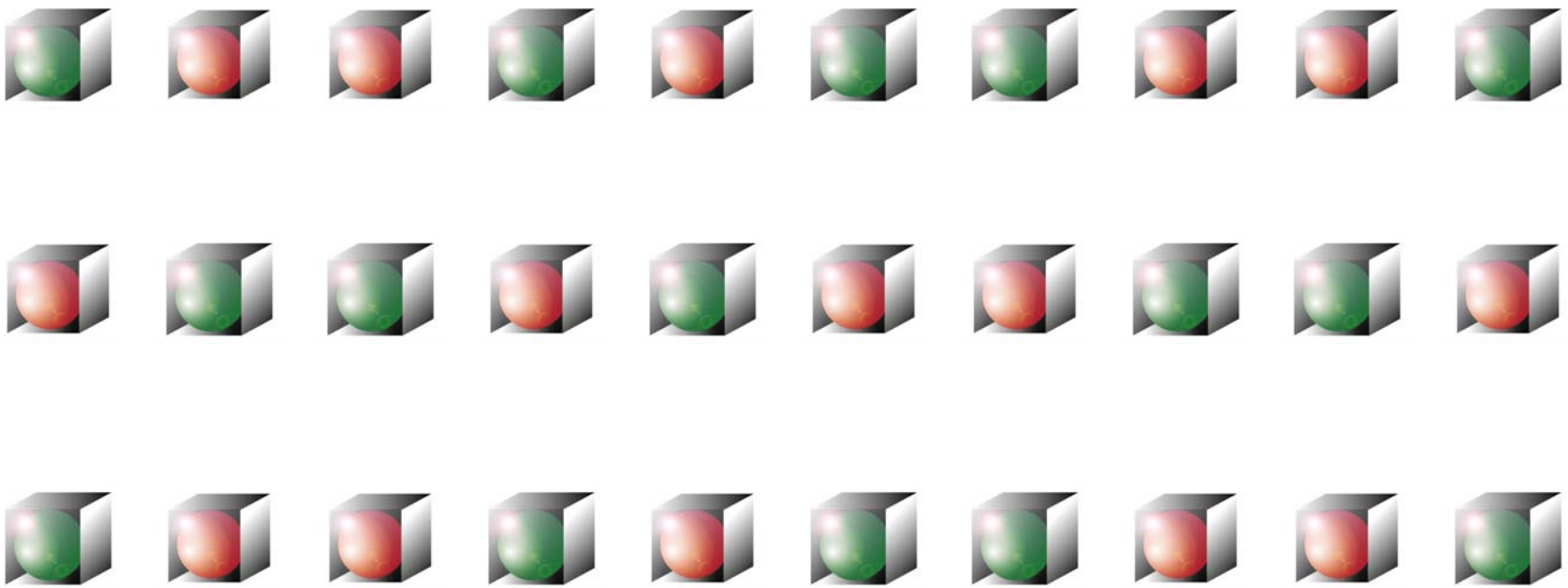
1,000 numbers to describe 10 qubits



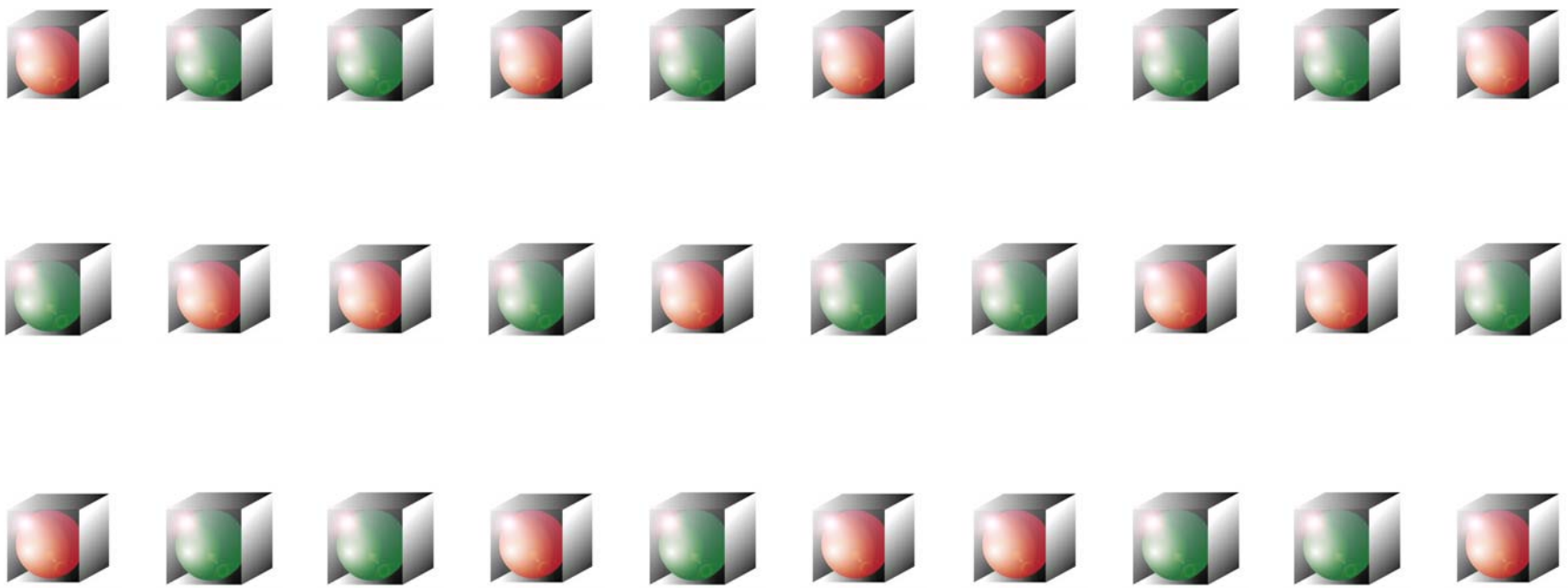
1,000,000 numbers to describe 20 qubits



1,000,000 numbers to describe 20 qubits



1,000,000,000 numbers to describe 30 qubits

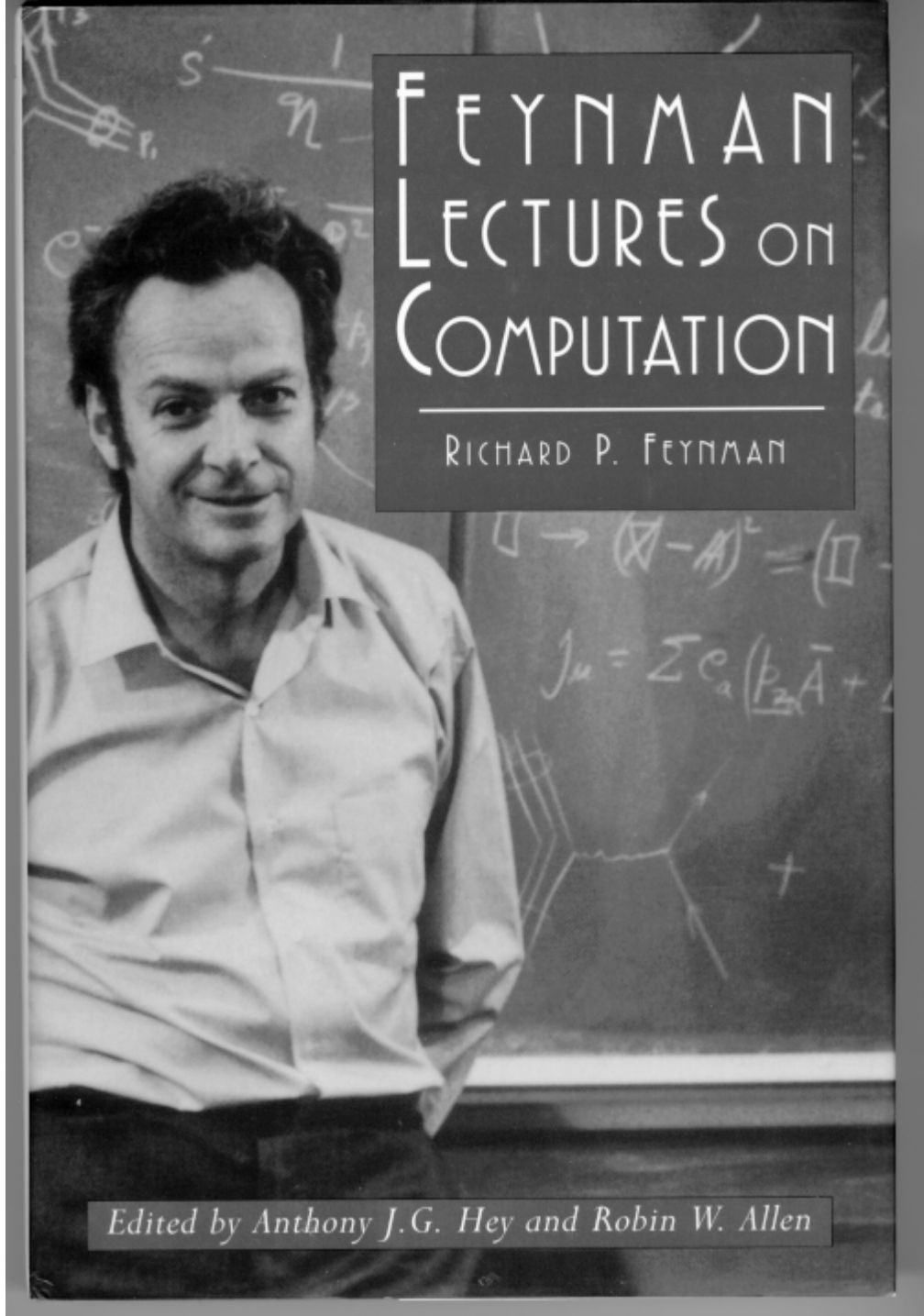


1,000,000,000 numbers to describe 30 qubits

To describe 300 qubits, we would need more numbers than the number of atoms in the visible universe!

We can't even hope to *describe* the state of a few hundred qubits in terms of classical bits.

Might a computer that operates on qubits rather than bits (a *quantum computer*) be able to perform tasks that are beyond the capability of any conceivable classical computer?



Prime Numbers

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,
43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

Finding Prime Factors

$$15 = \ ? \times \ ?$$

Finding Prime Factors

$$15 = 3 \times 5$$

Finding Prime Factors

$$91 = \ ? \times \ ?$$

Finding Prime Factors

$$91 = 7 \times 13$$

Finding Prime Factors

$$2537 = \; ? \times \; ?$$

Finding Prime Factors

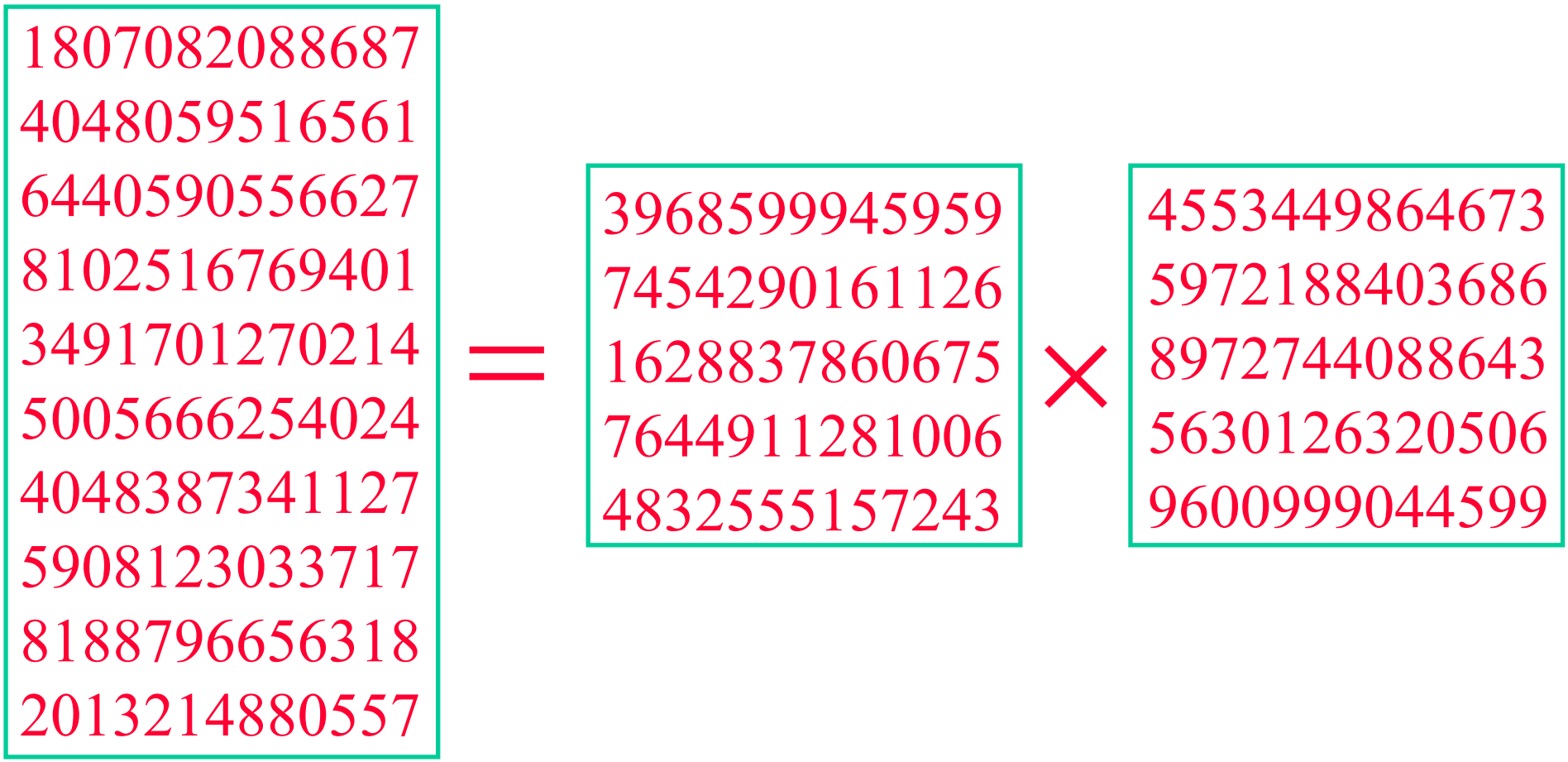
$$2537 = 43 \times 59$$

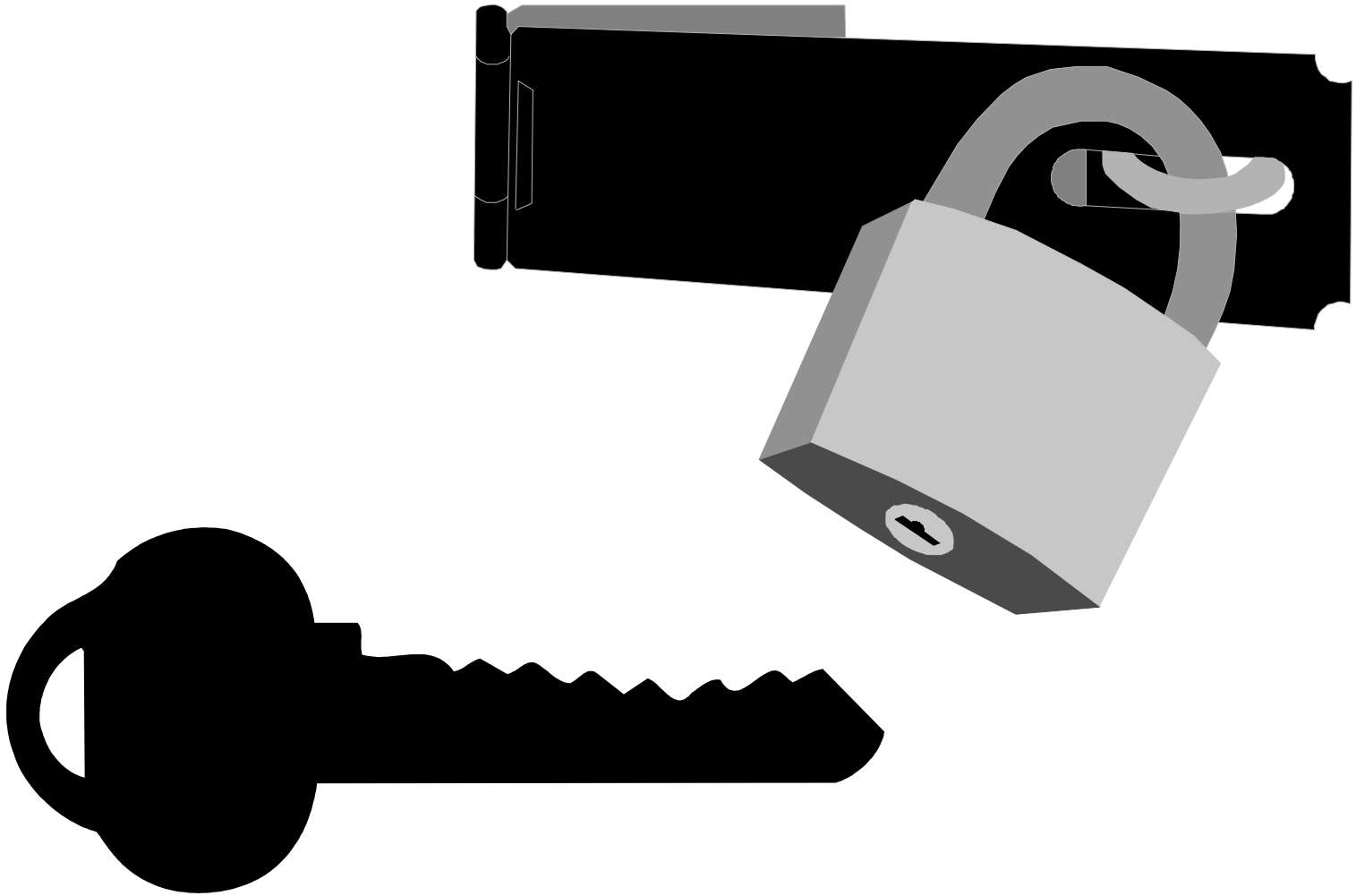
Finding Prime Factors

1807082088687
4048059516561
6440590556627
8102516769401
3491701270214
5005666254024
4048387341127
5908123033717
8188796656318
2013214880557

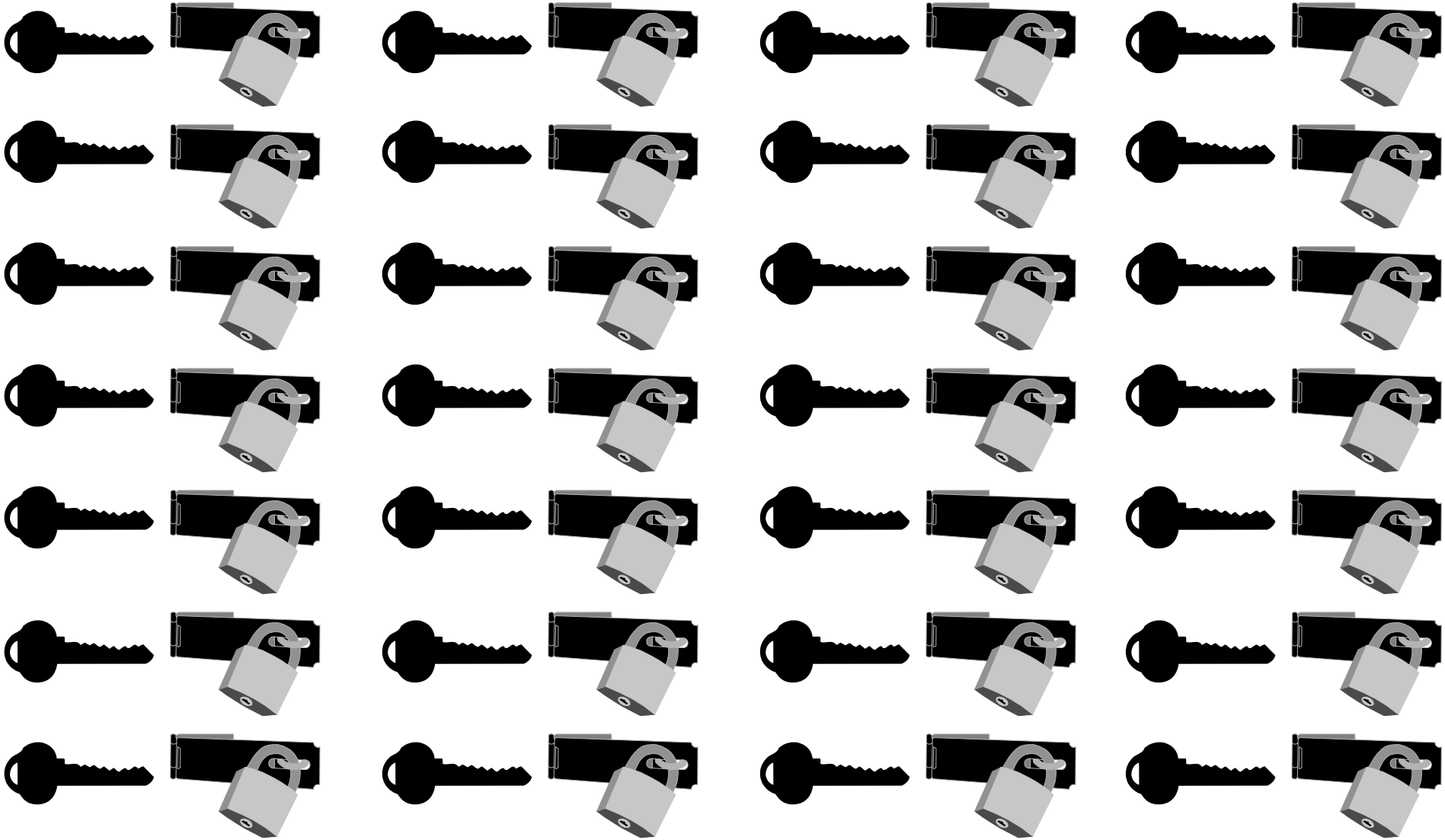
$= ? \times ?$

Finding Prime Factors





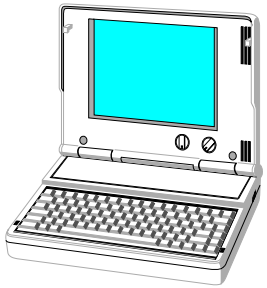
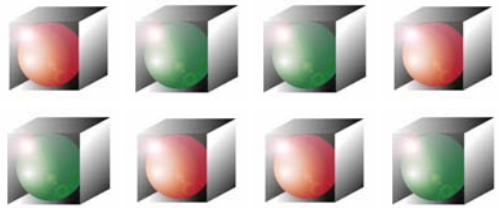
Try every key, until one fits the lock.



Try all the keys at once!

Massive

Parallelism

Classical Computer	Quantum Computer
	
Factor 193 digits in 30 CPU years (2.2 GHz).	Factor 193 digits in 1 second.
Factor 500 digits in 10^{12} CPU years.	Factor 500 digits in 20 seconds.
MISSION: IMPOSSIBLE	 Peter Shor (1994)

Finding Prime Factors

1807082088687
4048059516561
6440590556627
8102516769401
3491701270214
5005666254024
4048387341127
5908123033717
8188796656318
2013214880557

$= ? \times ?$

Finding Prime Factors

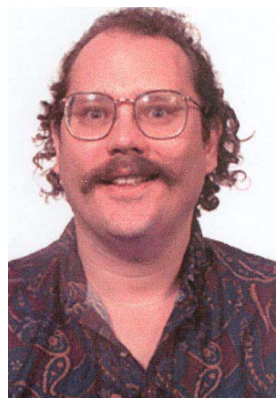
1807082088687
4048059516561
6440590556627
8102516769401
3491701270214
5005666254024
4048387341127
5908123033717
8188796656318
2013214880557

=

3968599945959
7454290161126
1628837860675
7644911281006
4832555157243

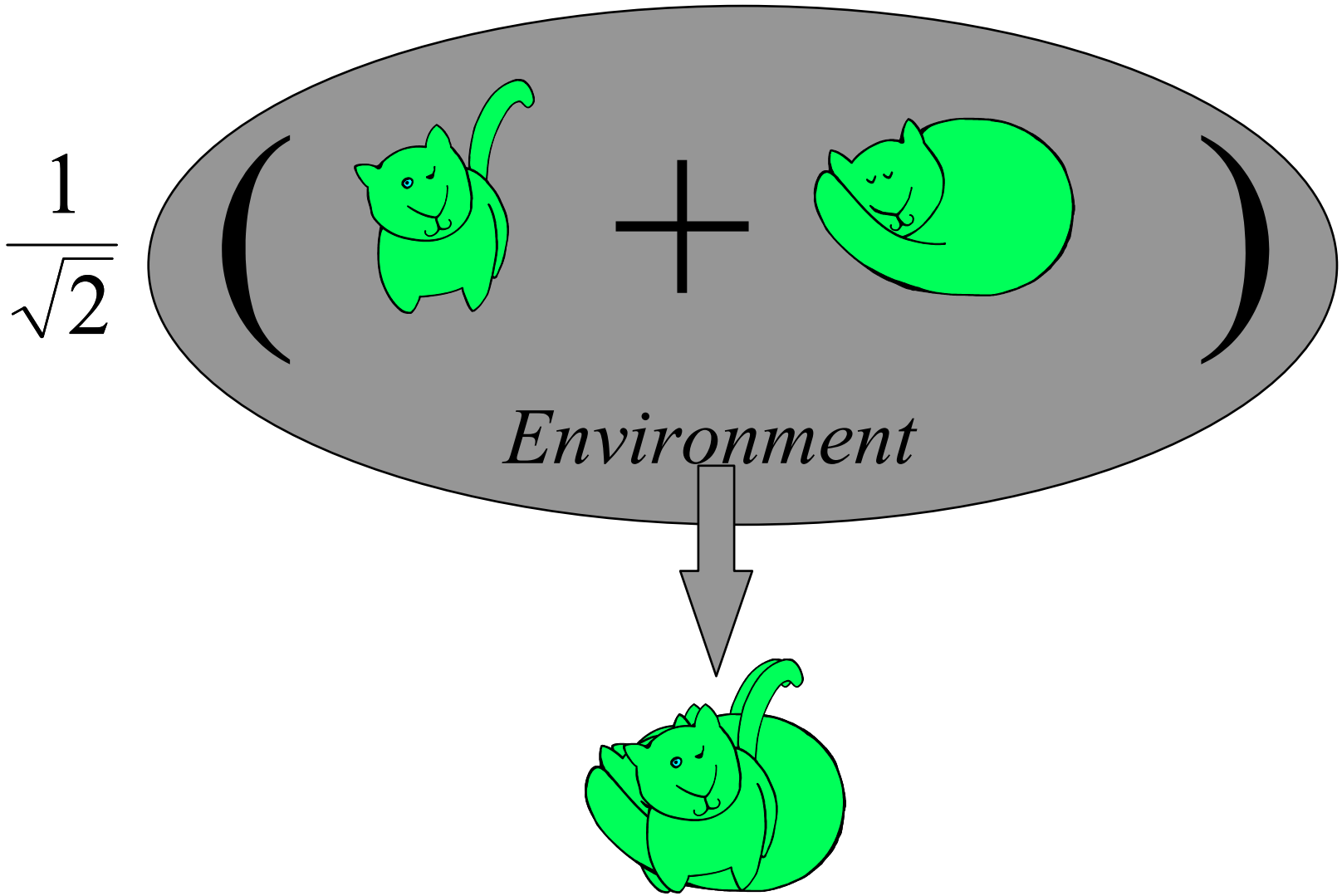
×

4553449864673
5972188403686
8972744088643
5630126320506
9600999044599

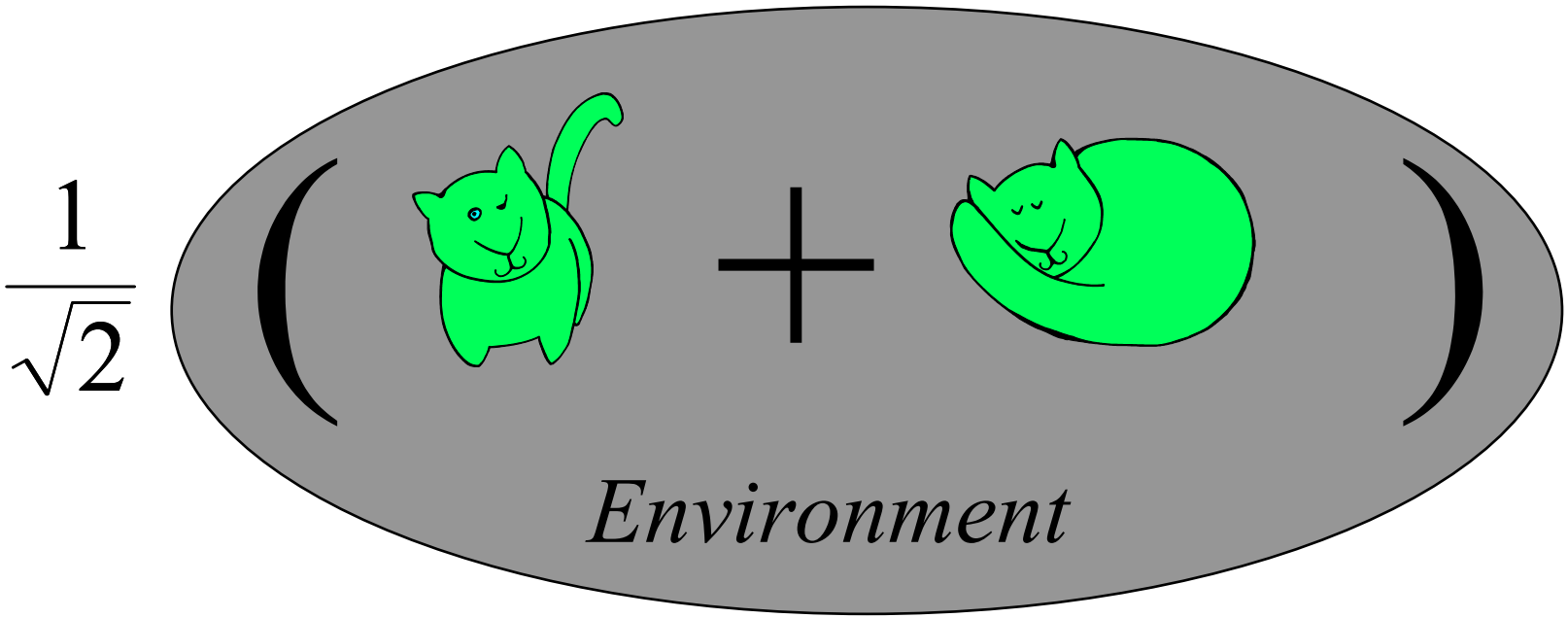


Shor ‘94

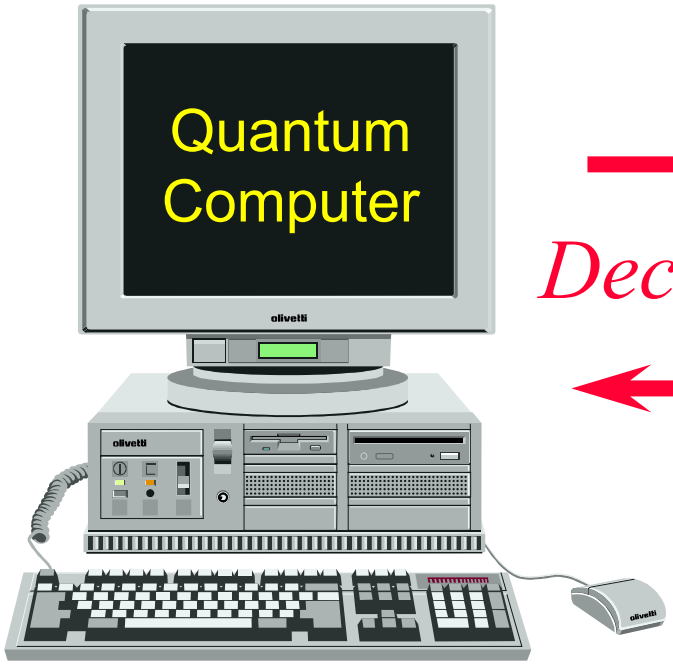
Decoherence



Decoherence



Decoherence explains why quantum phenomena, though observable in the microscopic systems studied in the physics lab, are not manifest in the macroscopic physical systems that we encounter in our ordinary experience.



Decoherence

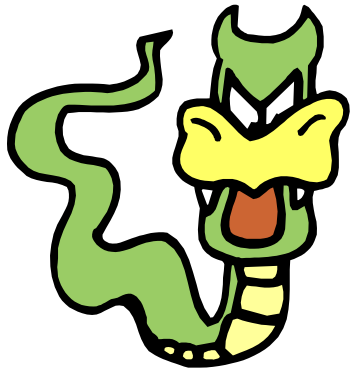
Environment

ERROR!

How can we protect a quantum computer from decoherence and other sources of error?

What about errors?

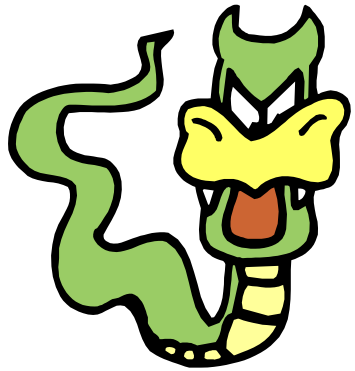
What about errors?



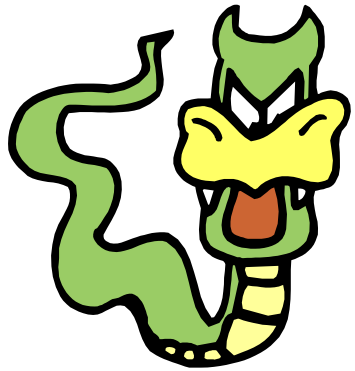
What about errors?

Error!

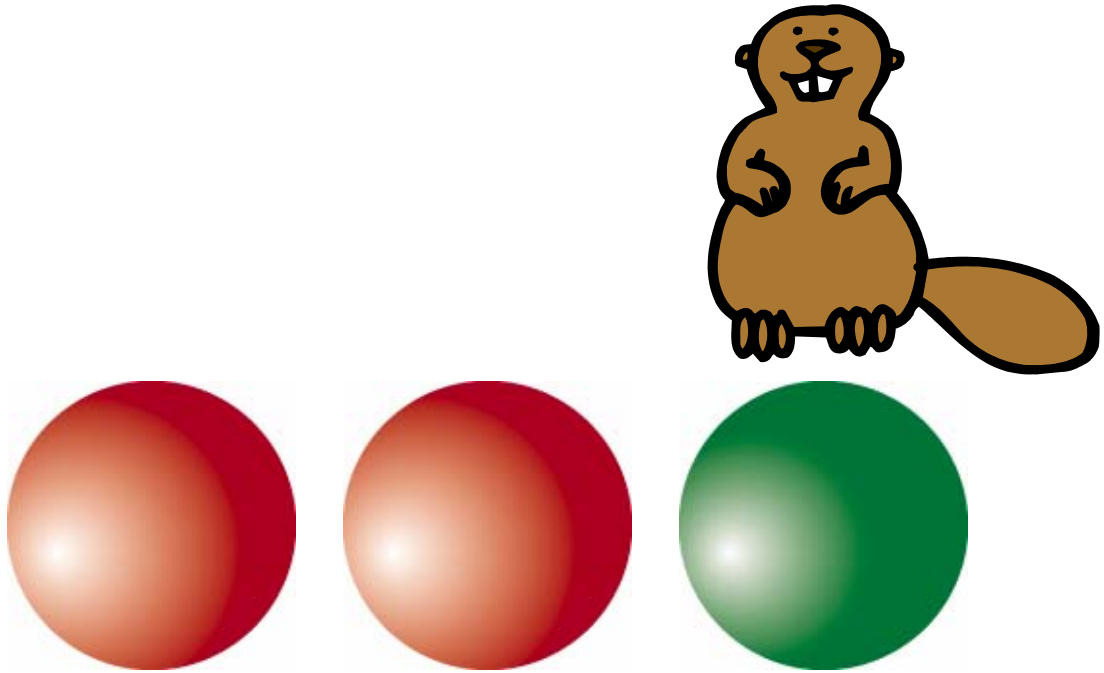
What about errors?



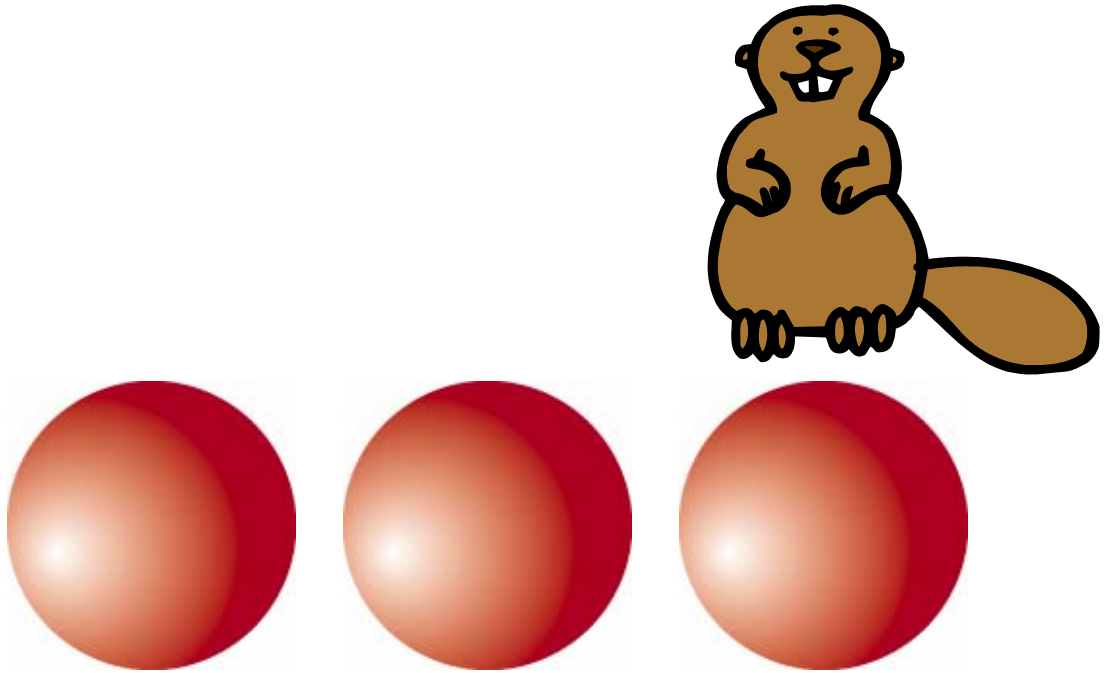
What about errors?



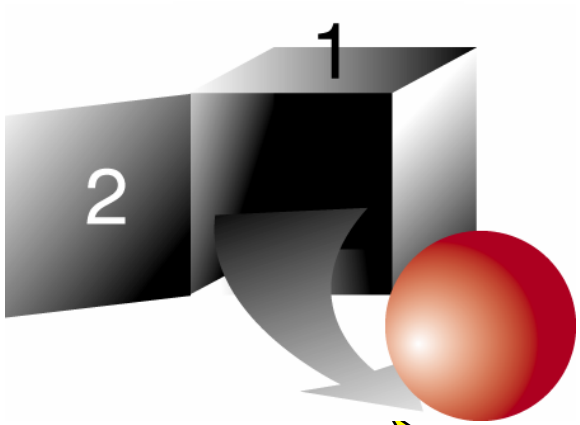
What about errors?

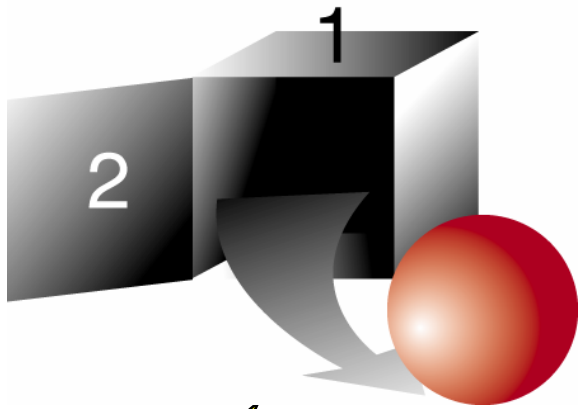


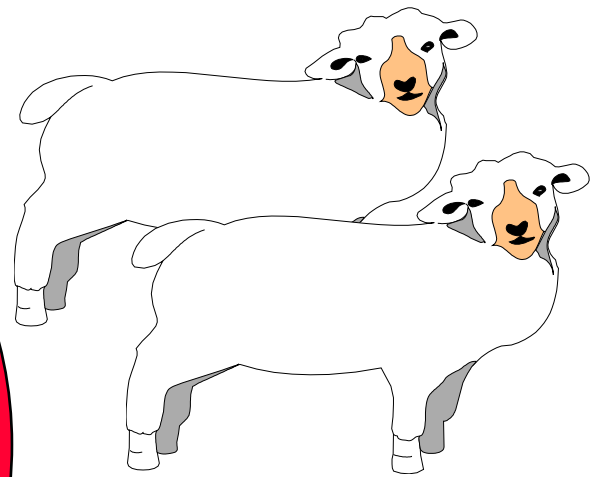
What about errors?



Redundancy protects against errors.

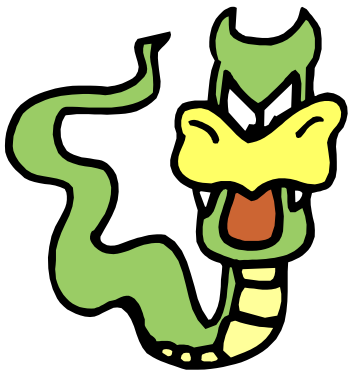


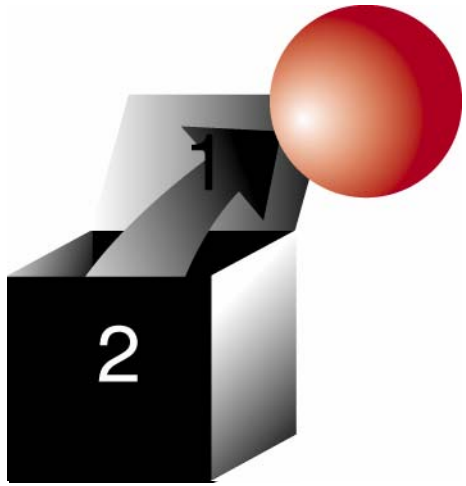




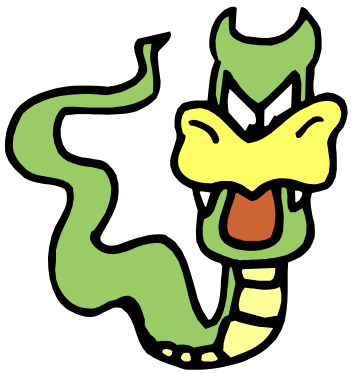
No cloning!

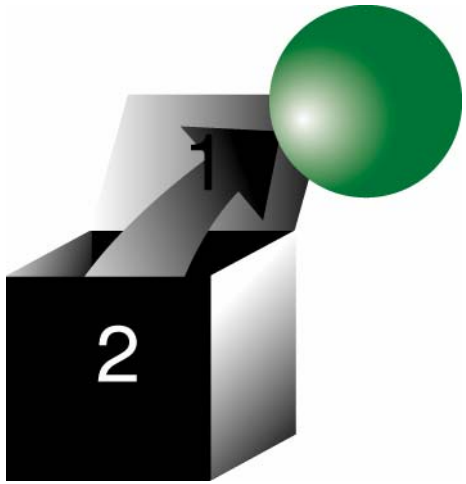
What about *quantum* errors?



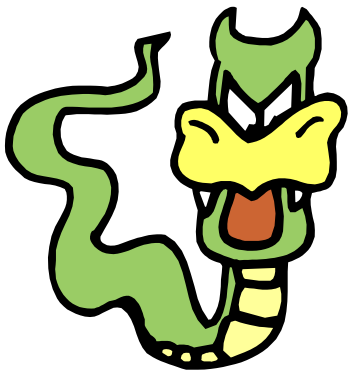


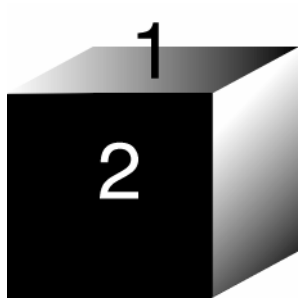
What about *quantum* errors?





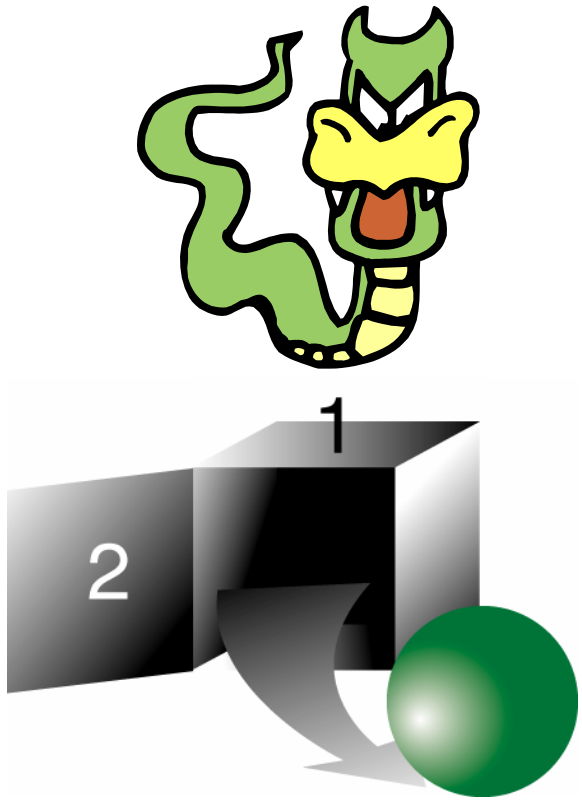
What about *quantum* errors?



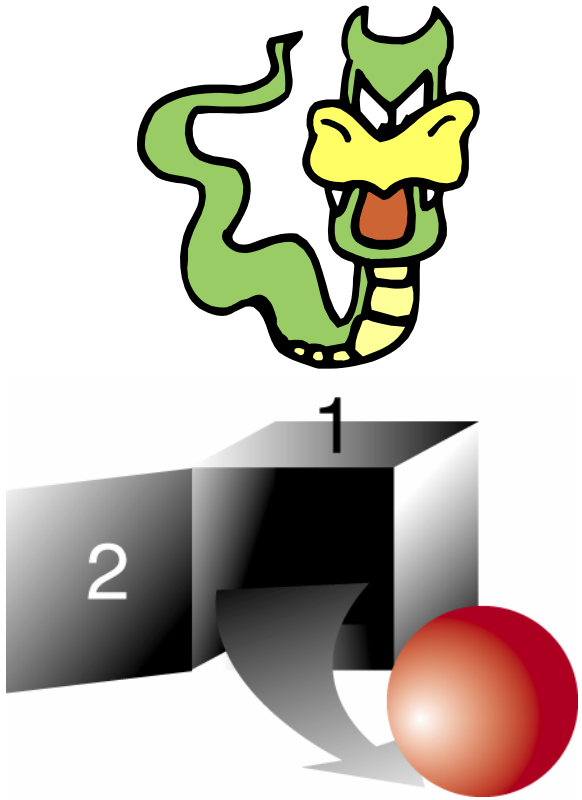


Error!

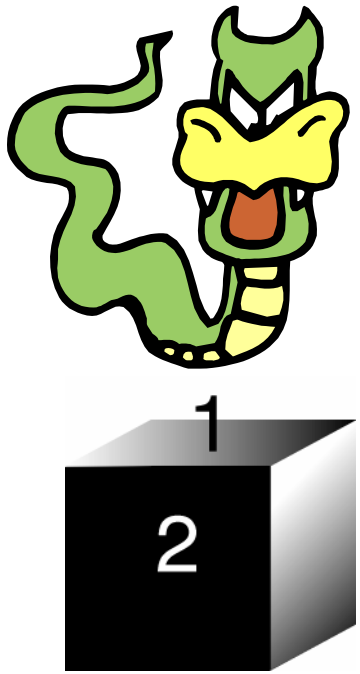
What about *quantum* errors?



What about *quantum* errors?

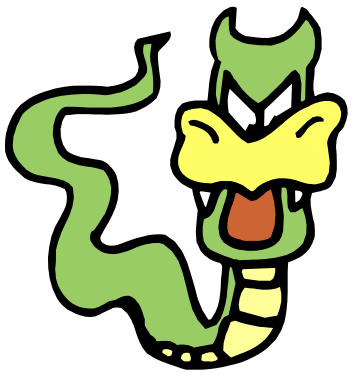


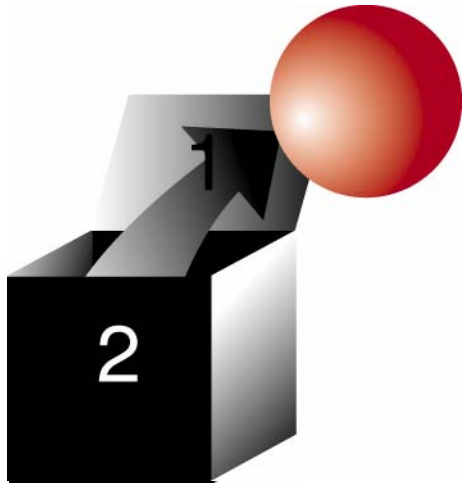
What about *quantum* errors?



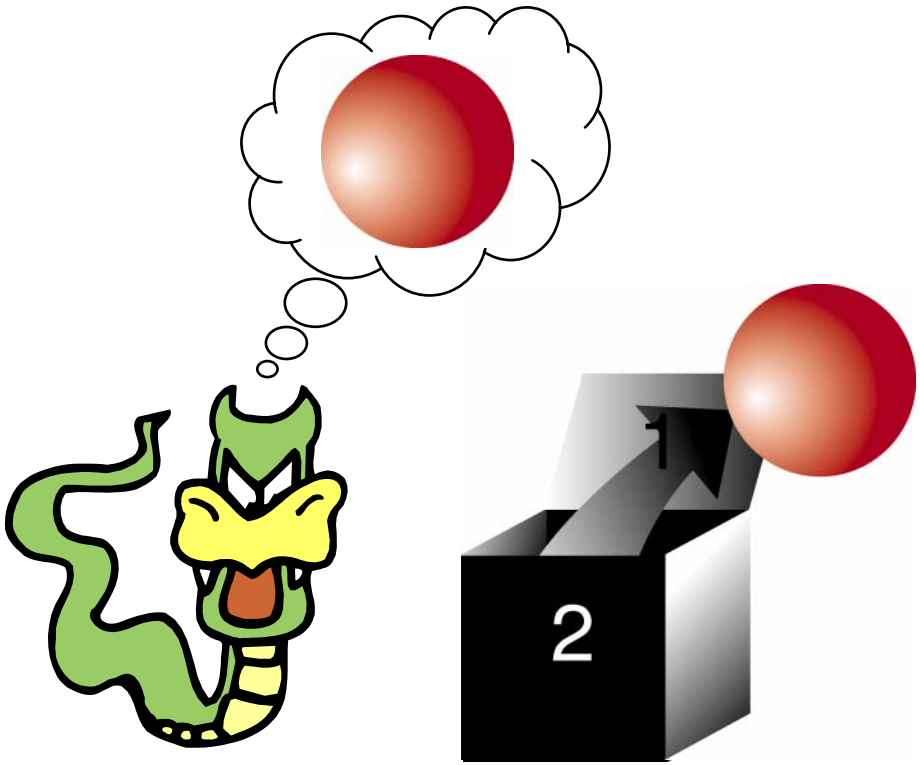
To fix the errors, must we know what door the dragon opened?

What about *quantum* errors?

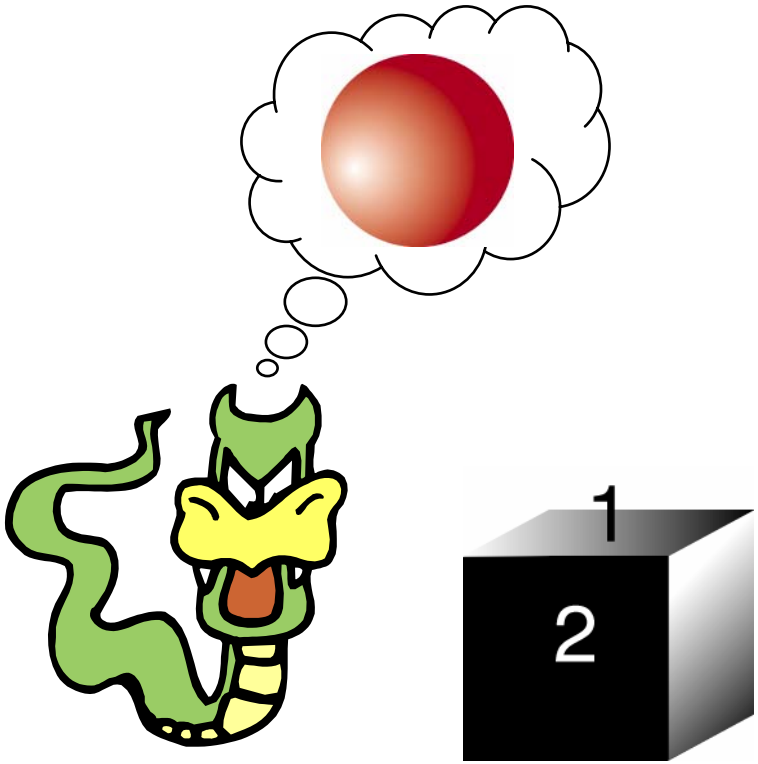




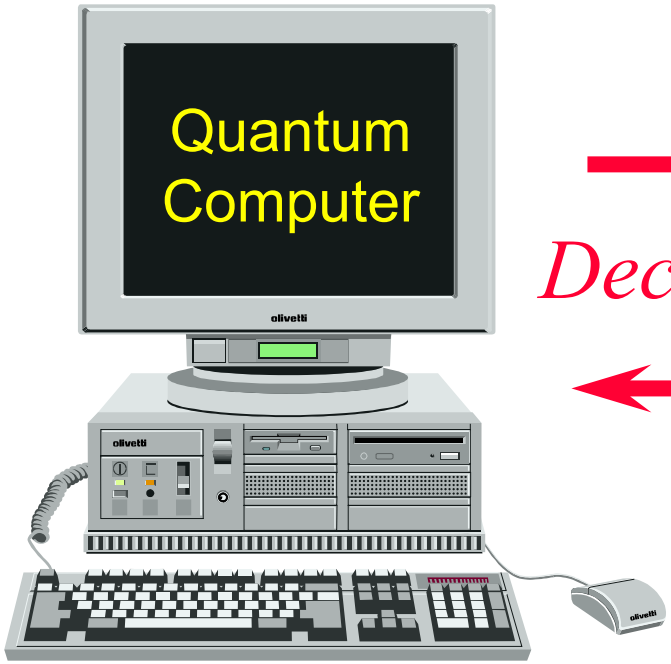
What about *quantum* errors?



What about *quantum* errors?



A door-number-2 error ("phase error") occurs if the dragon remembers (i.e., copies) the color that he sees through door number 1. It is easier to remember a bit than to flip a bit; therefore, phase errors are particularly pervasive.



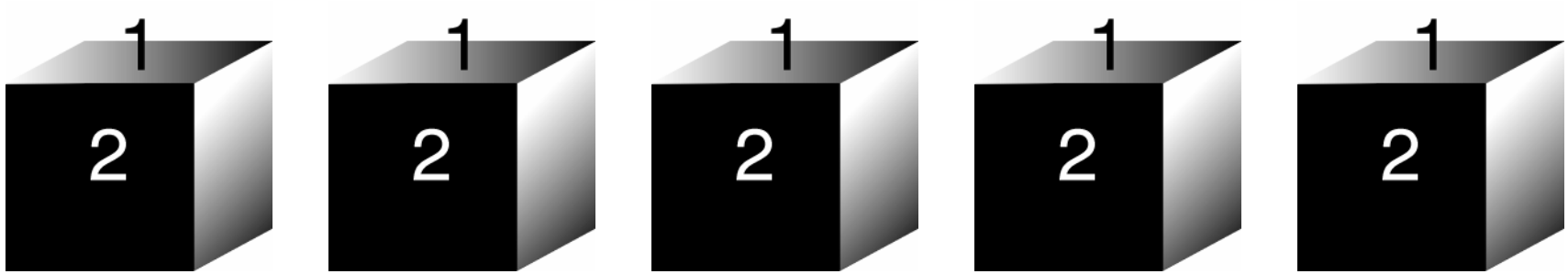
Decoherence

Environment

ERROR!

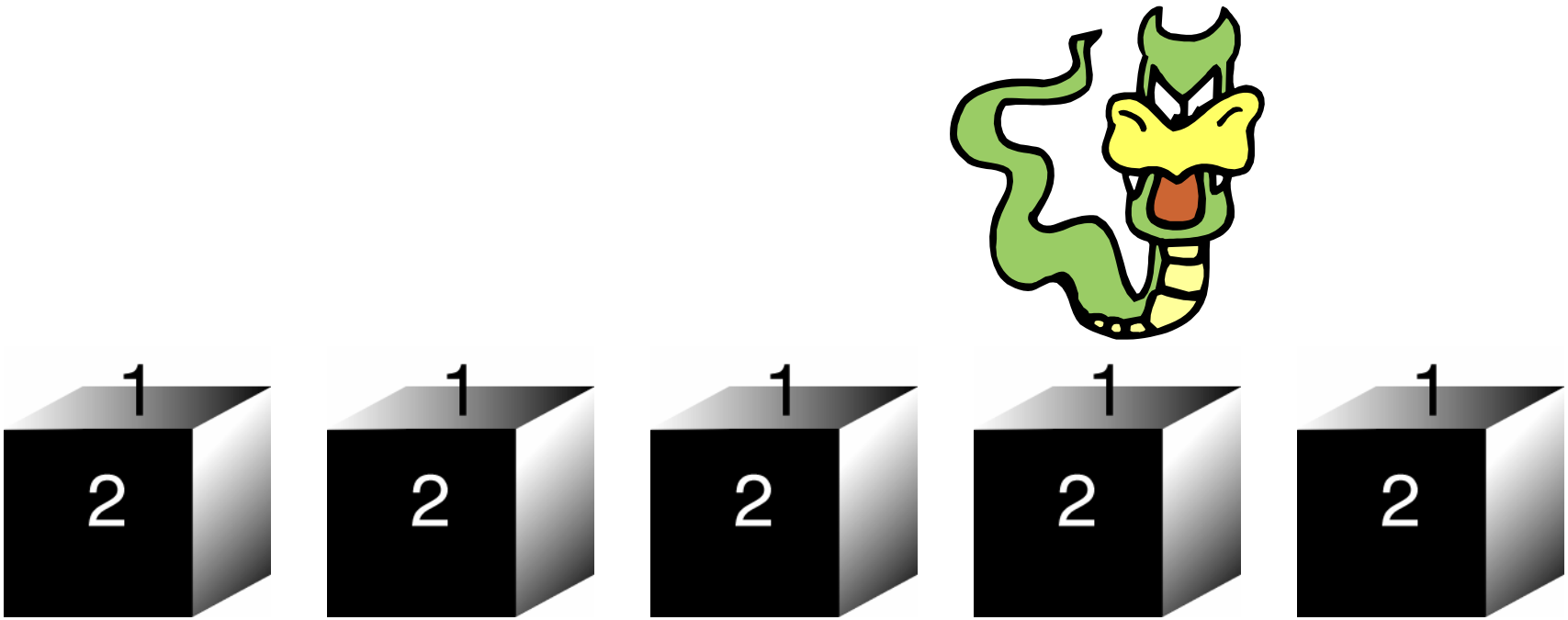
To resist decoherence, we must prevent the environment from "learning" about the state of the quantum computer during the computation.

What about *quantum* errors?

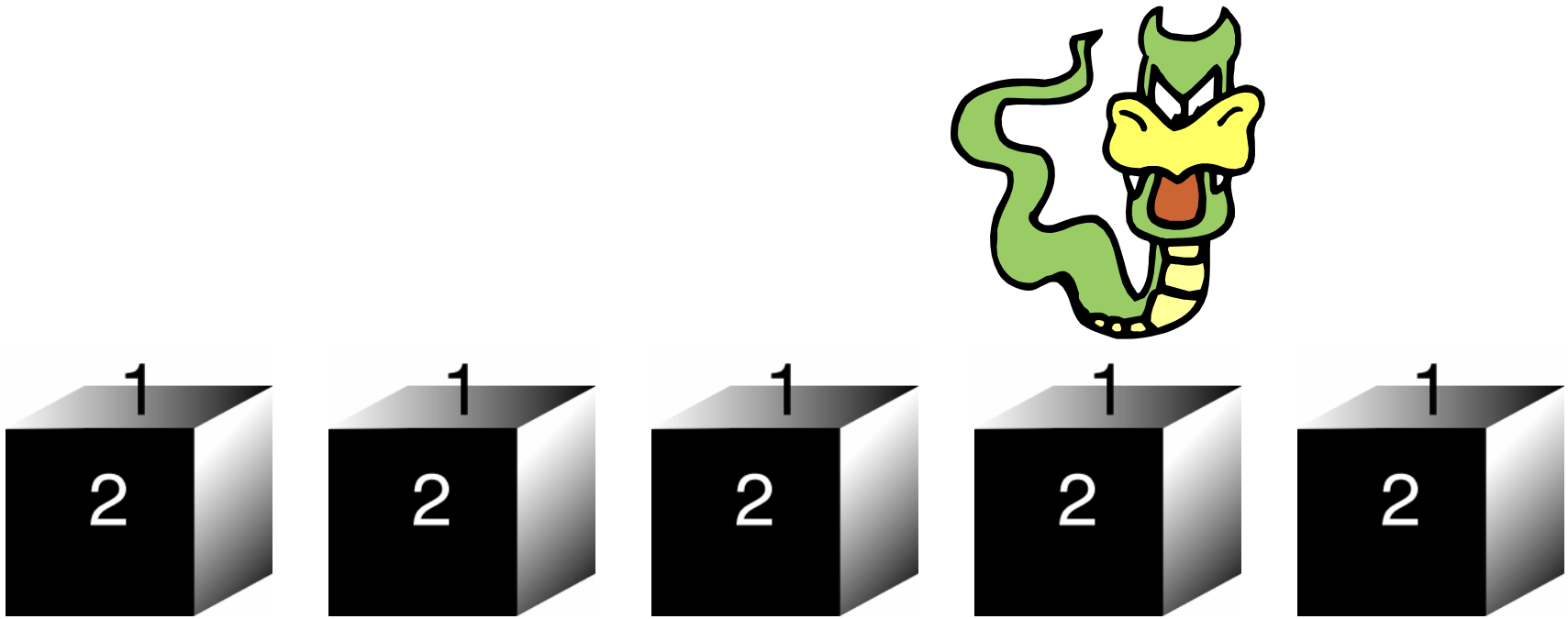


One qubit of quantum information can be encoded in the nonlocal correlations among five qubits.

What about *quantum* errors?

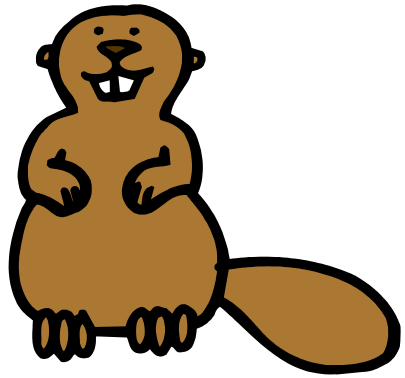


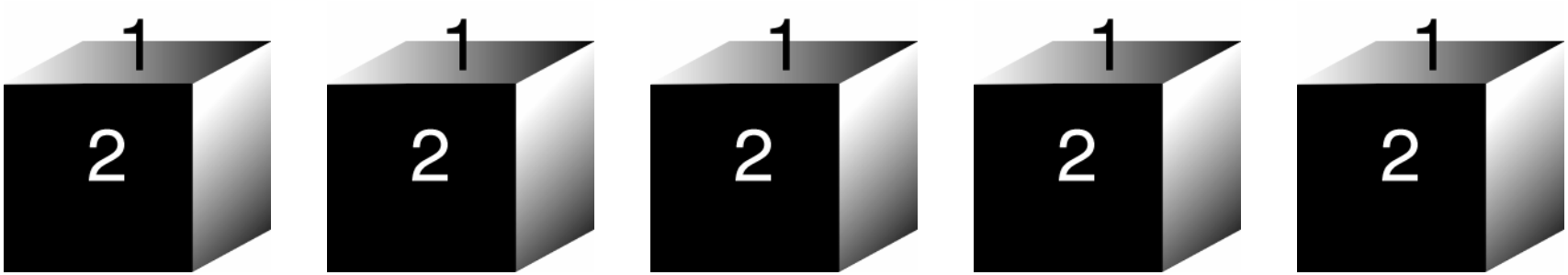
What about *quantum* errors?



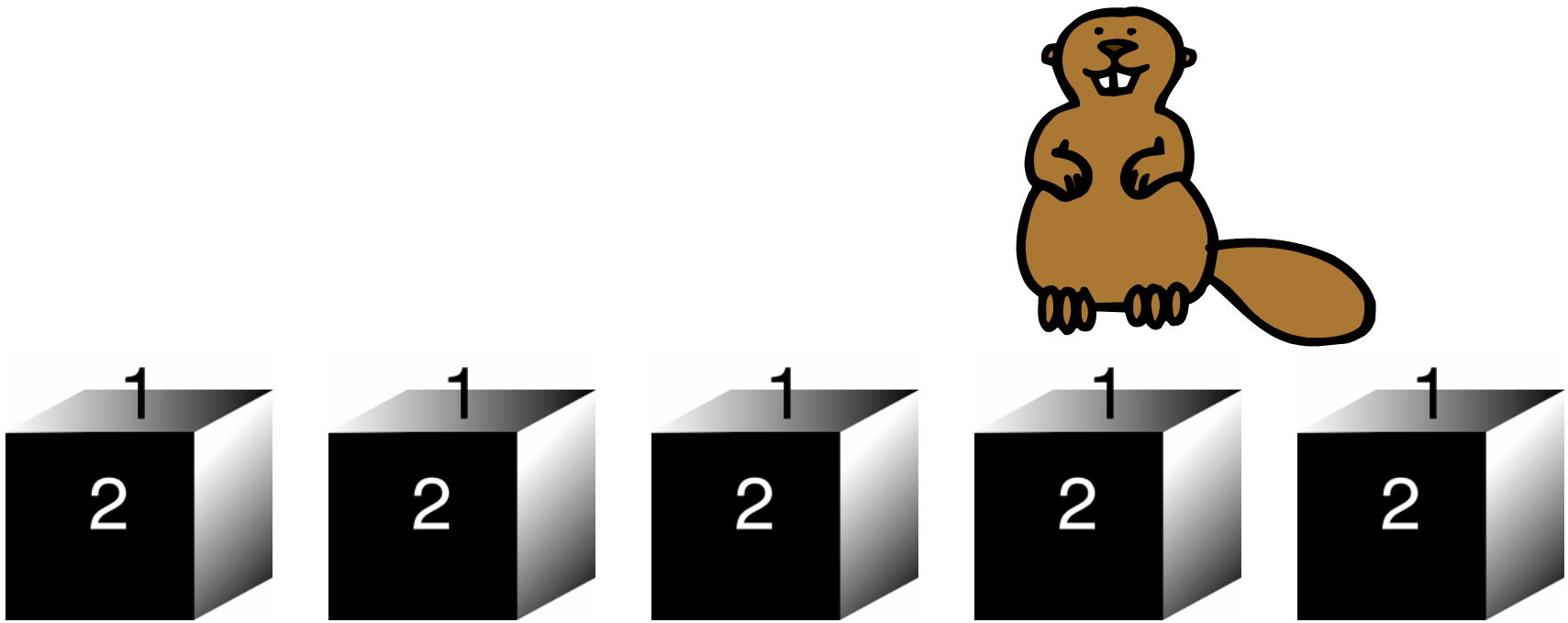
Though the dragon does damage one of the boxes, and he might learn something about the color of the ball in that box, this information does not tell him anything about the *encoded* qubit. Therefore the damage is *reversible*.

What about *quantum* errors?



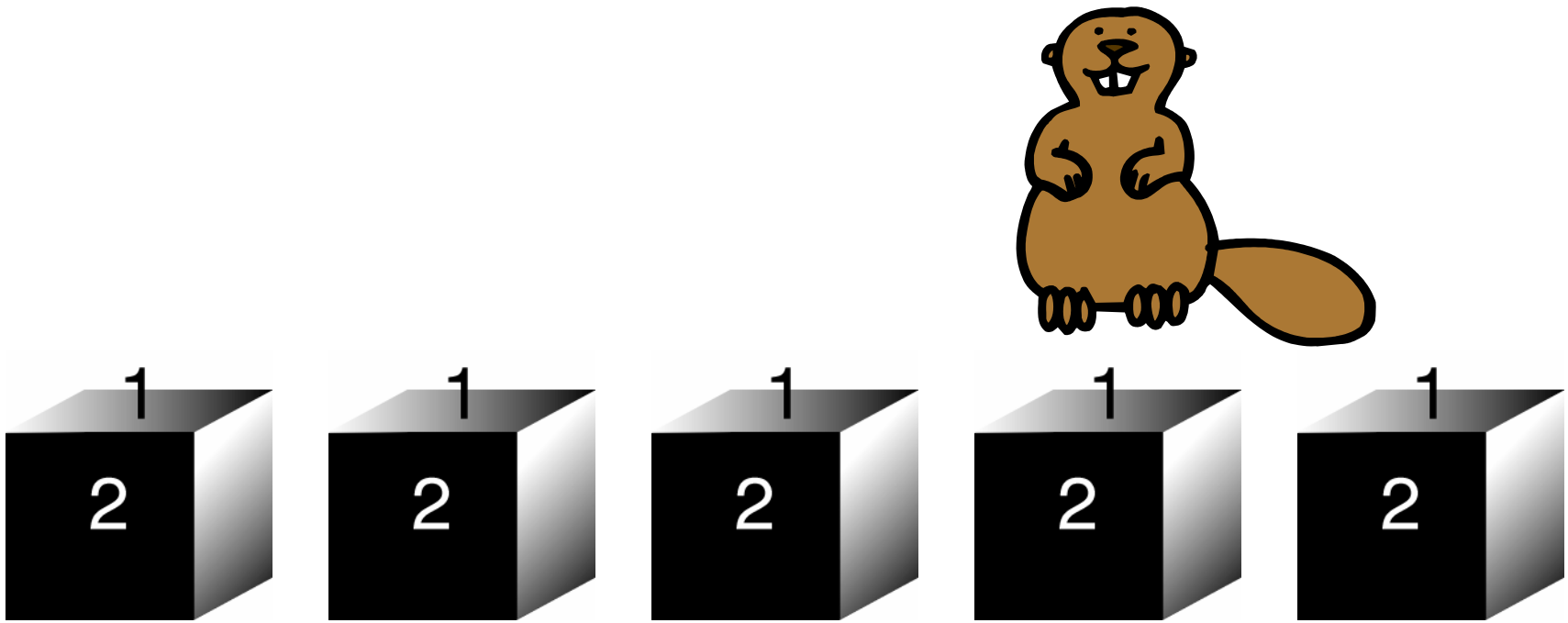


What about *quantum* errors?



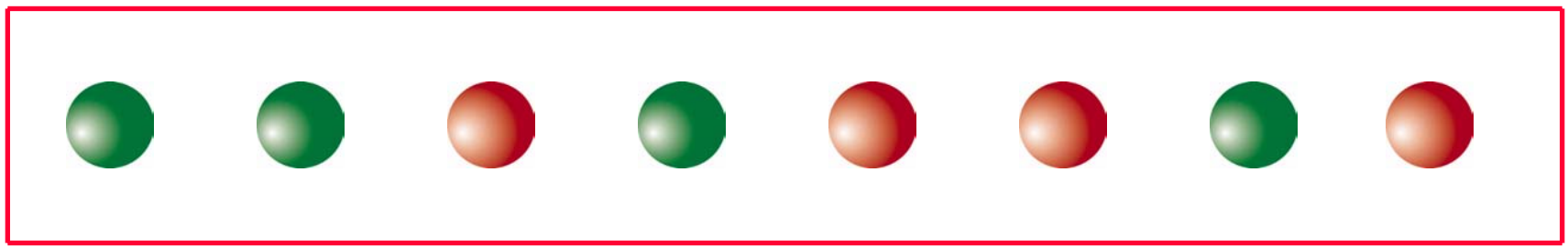
By making carefully designed *collective* measurements on the five qubits (using a quantum computer), the beaver learns what damage the dragon inflicted, and how to reverse it. But he, too, learns nothing about the state of the encoded qubit.

What about *quantum* errors?

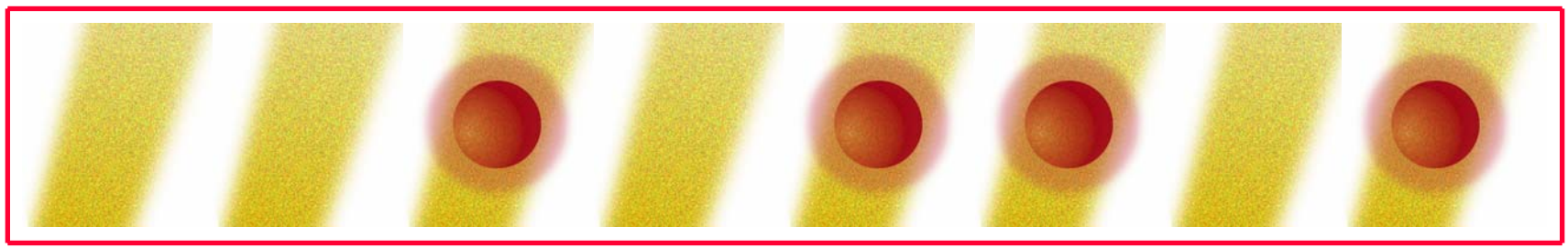


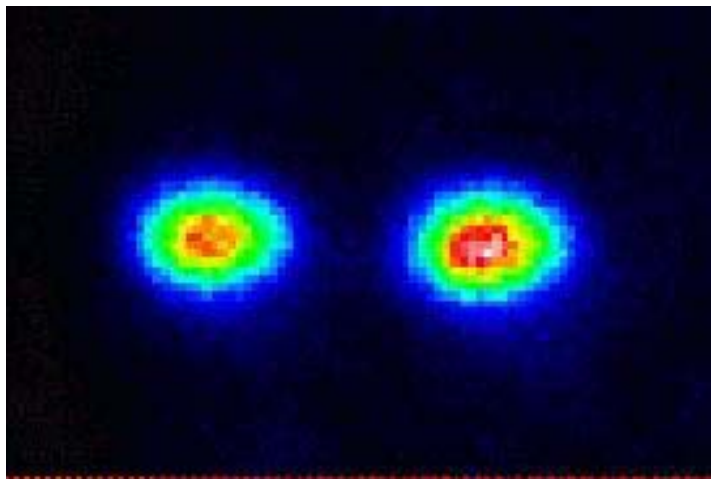
Redundancy protects against *quantum* errors!

Ion Trap Quantum Computer



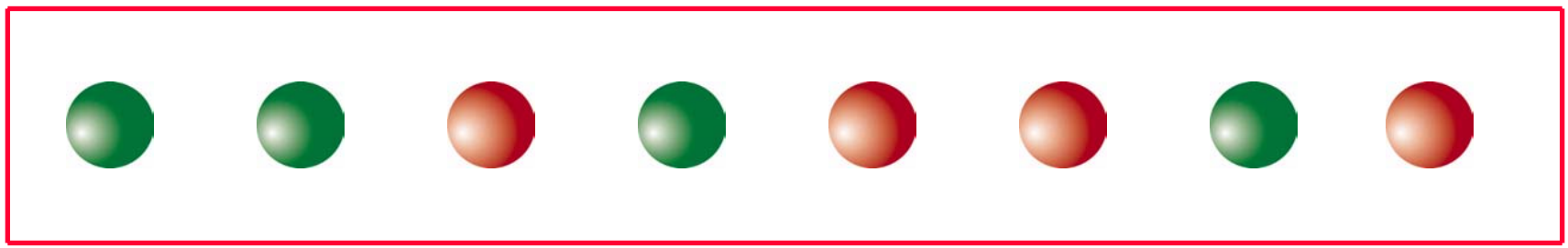
Ion Trap Quantum Computer



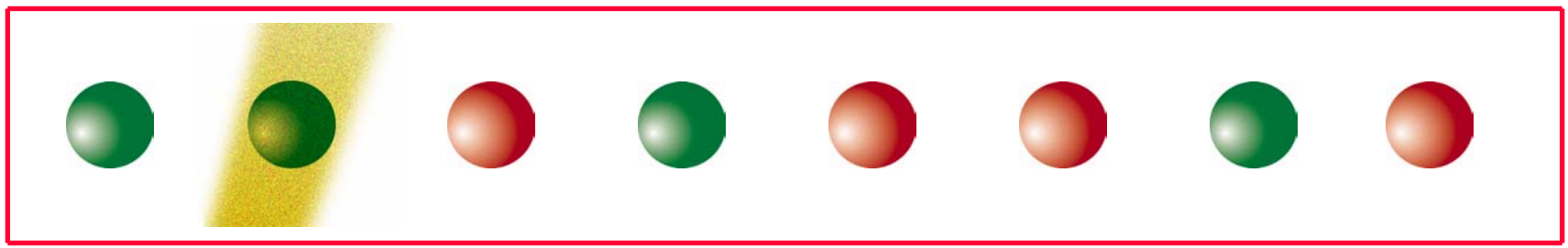


Two $^{9}Be^{+}$ ions in an ion trap at the National Institute of Standards and Technology (NIST) in Boulder, CO.

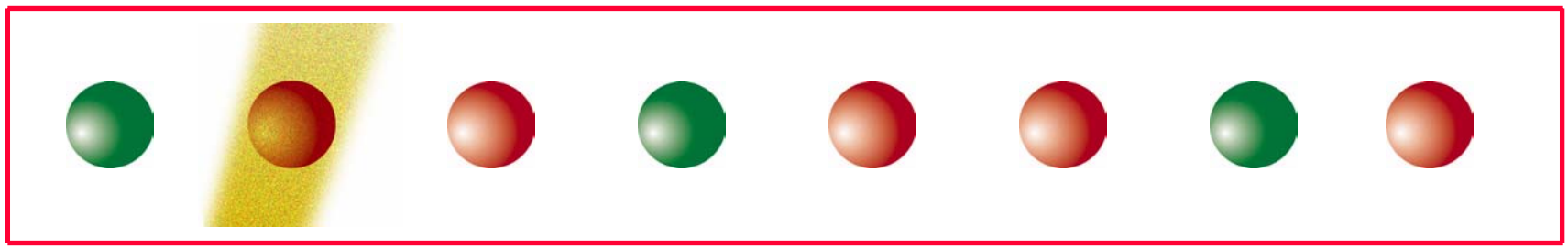
Ion Trap Quantum Computer



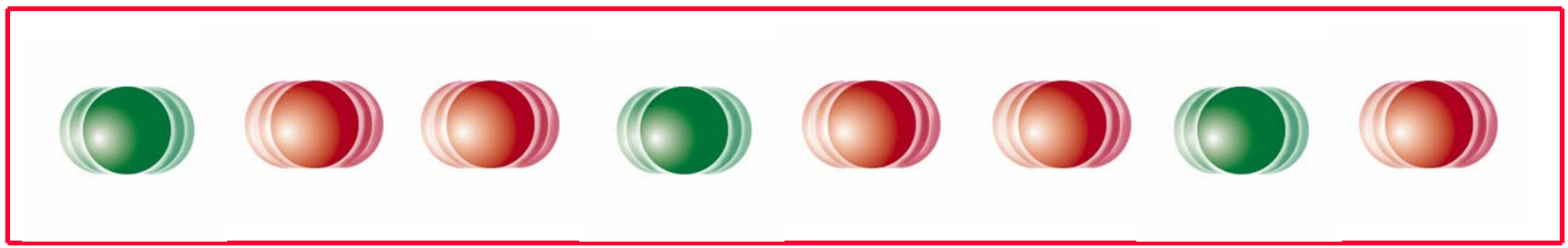
Ion Trap Quantum Computer



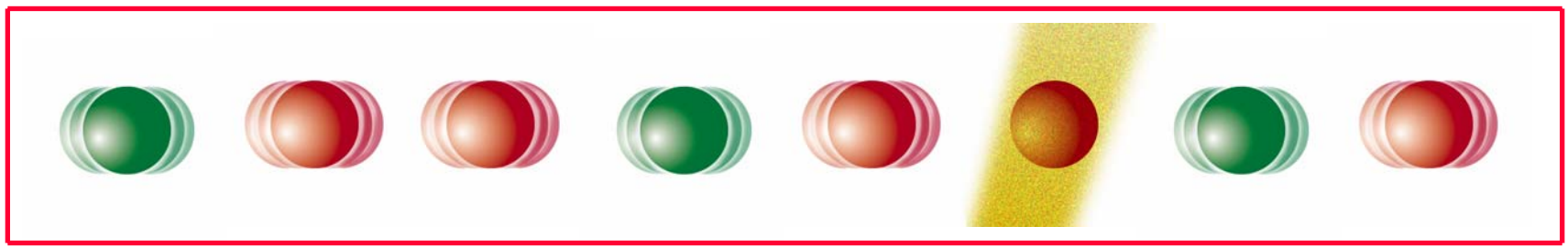
Ion Trap Quantum Computer



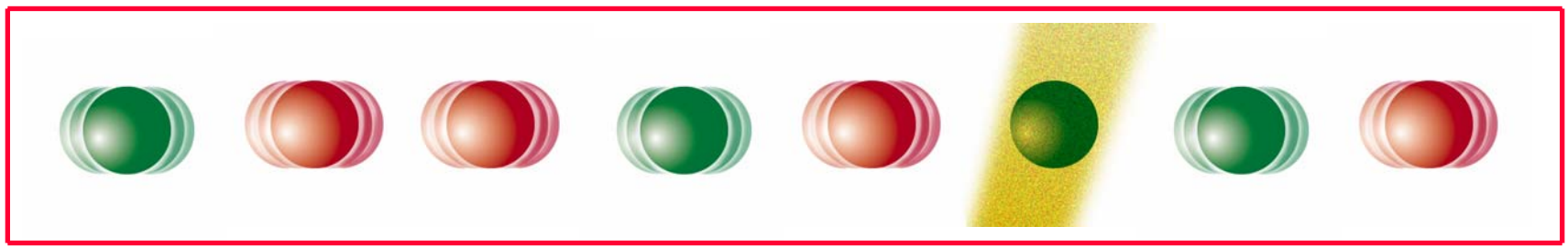
Ion Trap Quantum Computer



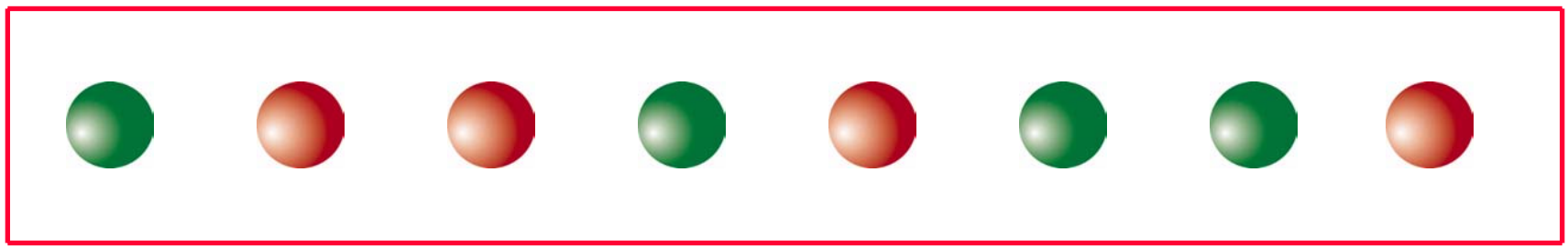
Ion Trap Quantum Computer



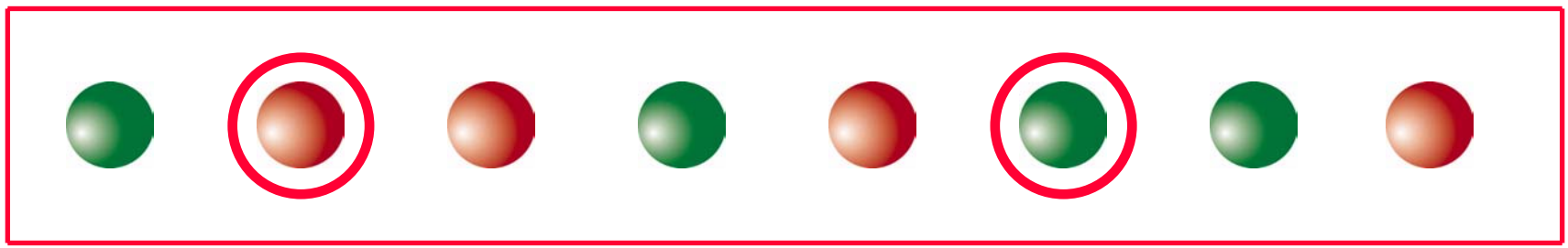
Ion Trap Quantum Computer



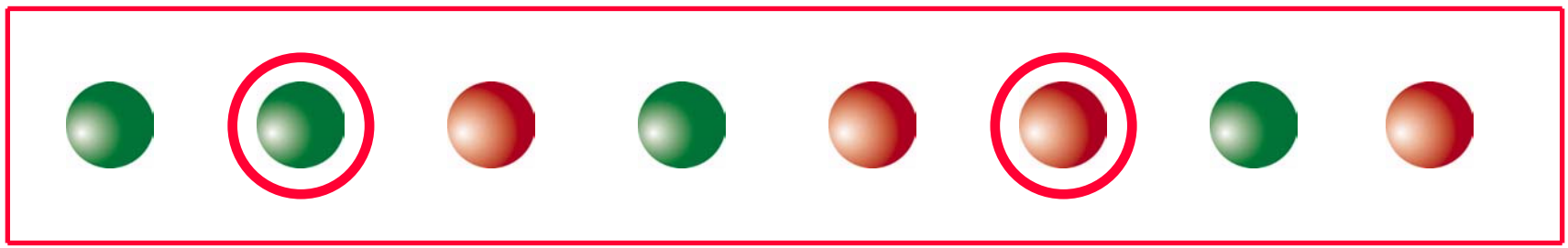
Ion Trap Quantum Computer



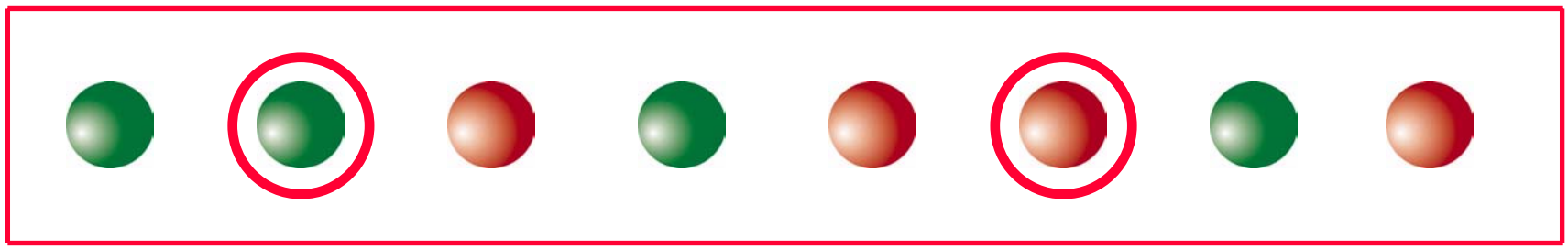
Ion Trap Quantum Computer



Ion Trap Quantum Computer

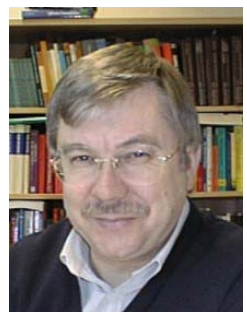


Ion Trap Quantum Computer

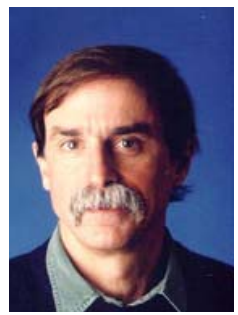


Cirac

Zoller

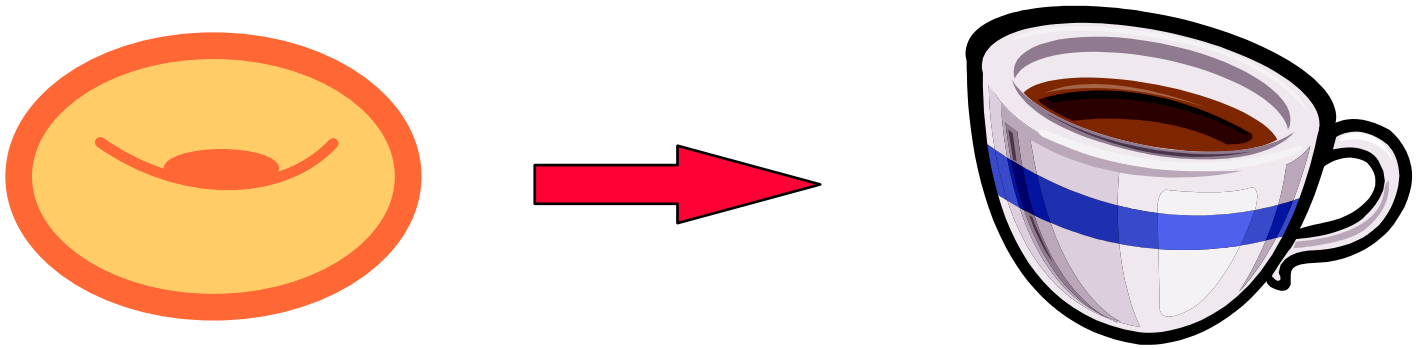


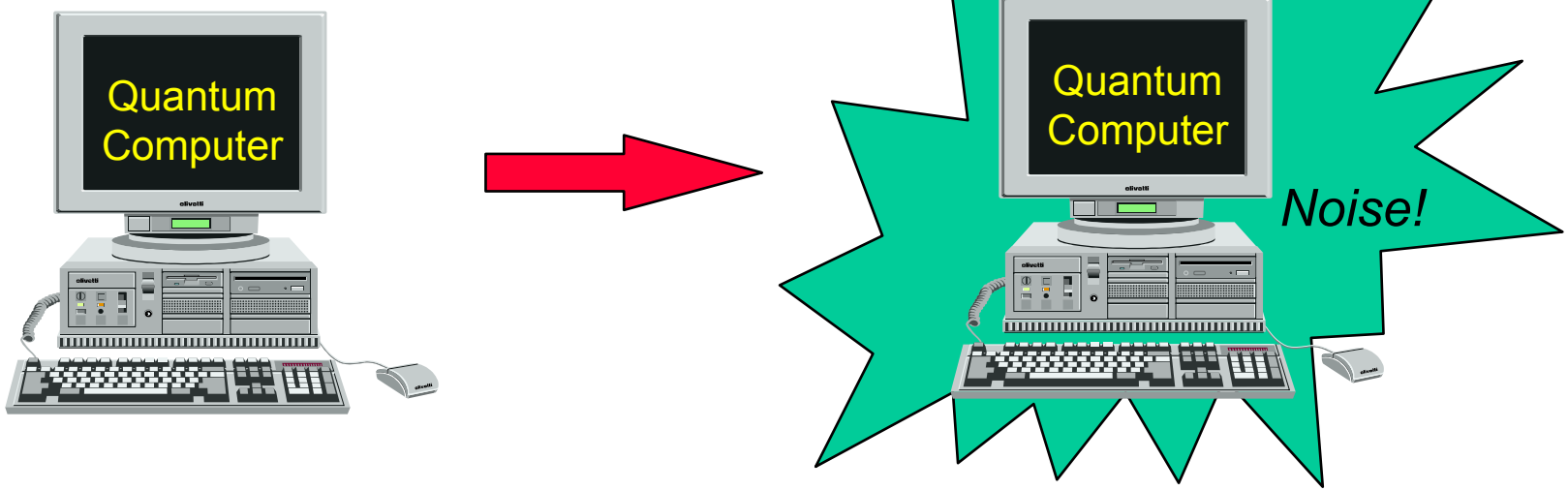
Blatt

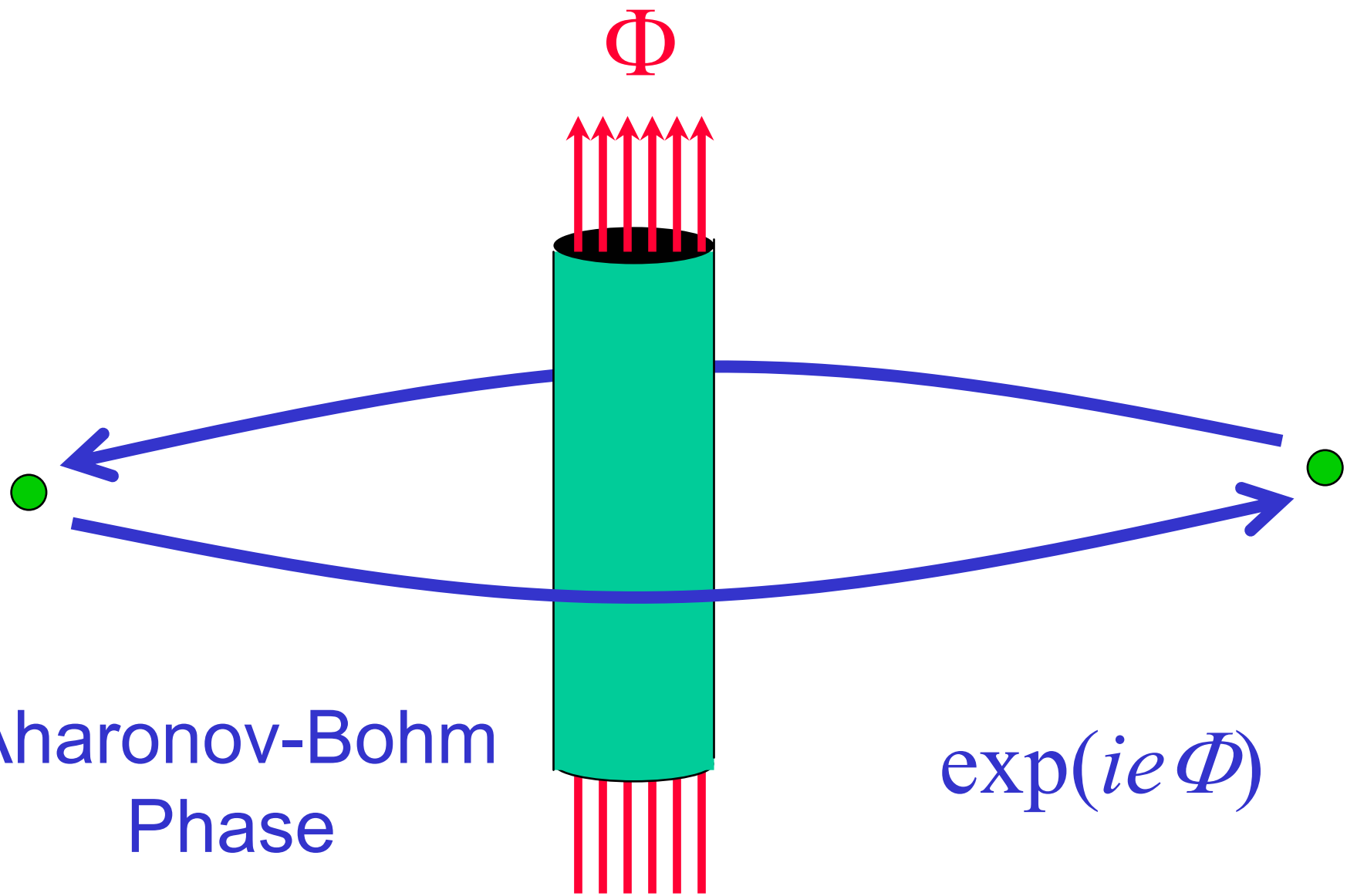


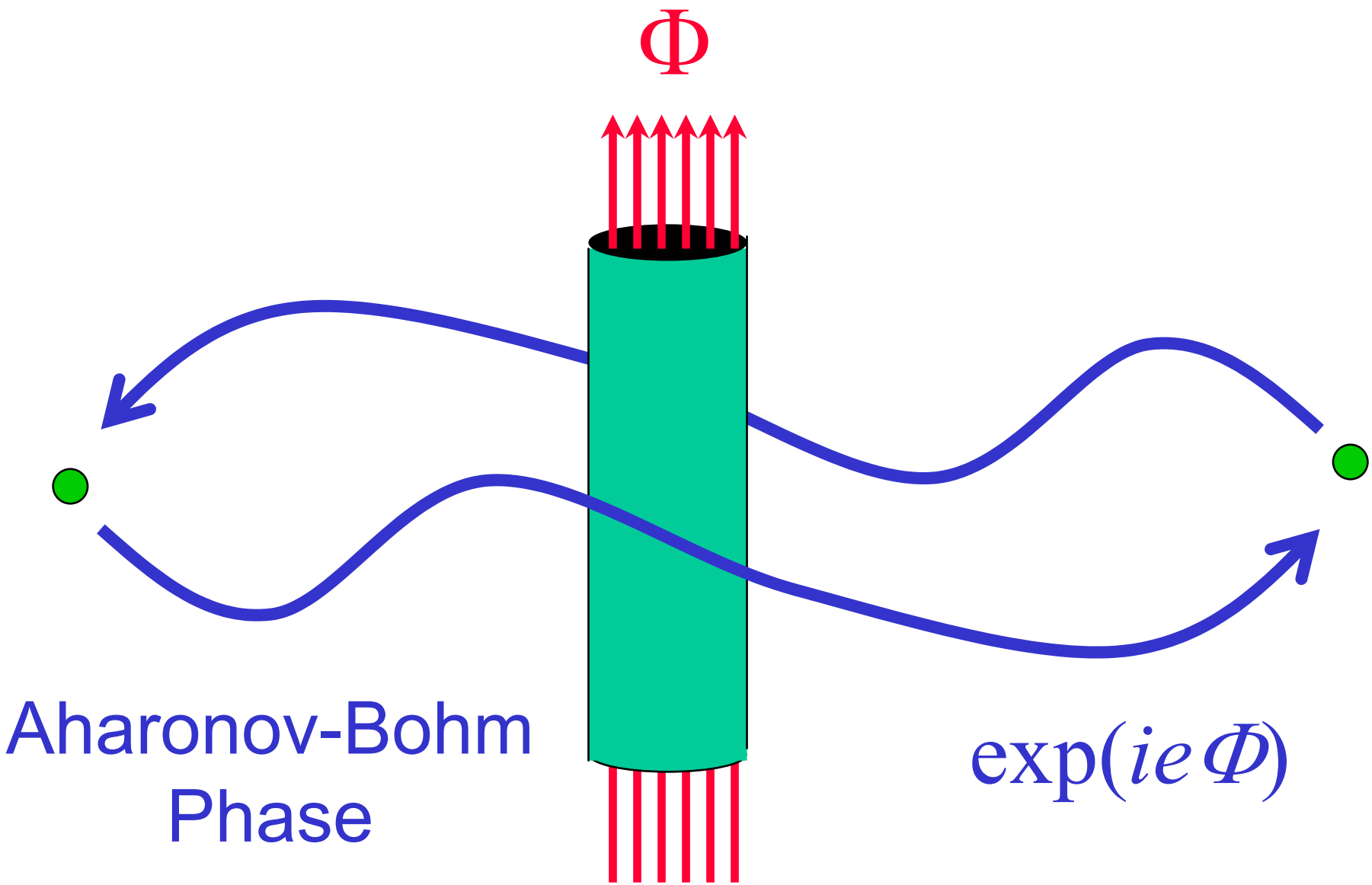
Wineland

Topology



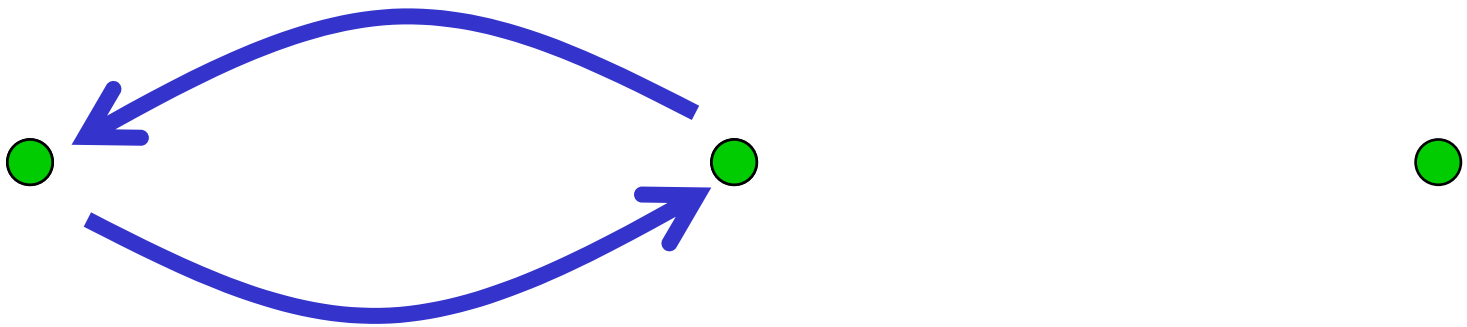



Φ
Aharonov-Bohm
Phase
exp(ieΦ)


Φ
Aharonov-Bohm
Phase
exp(ieΦ)

Anyons

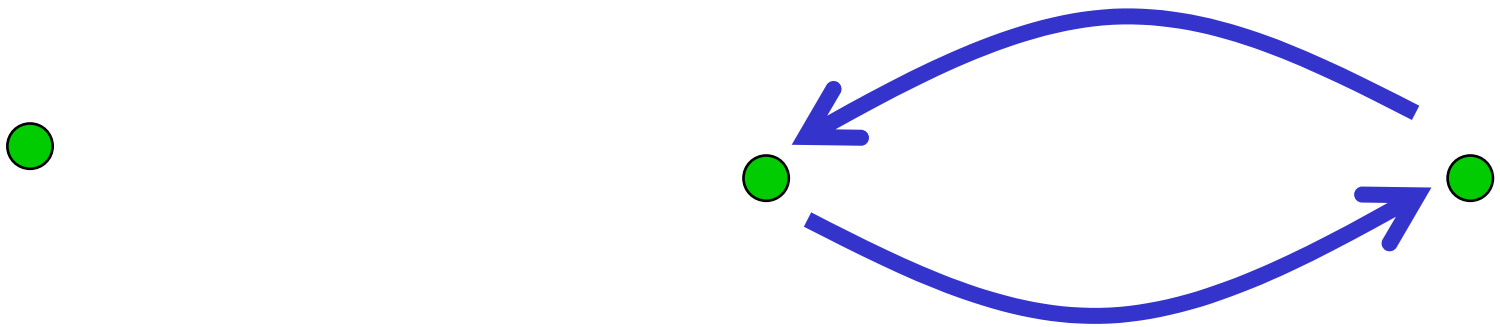
Quantum information can be stored in the collective state of exotic particles in two dimensions (“anyons”).



The information can be processed by exchanging the positions of the anyons (even though the anyons never come close to one another.

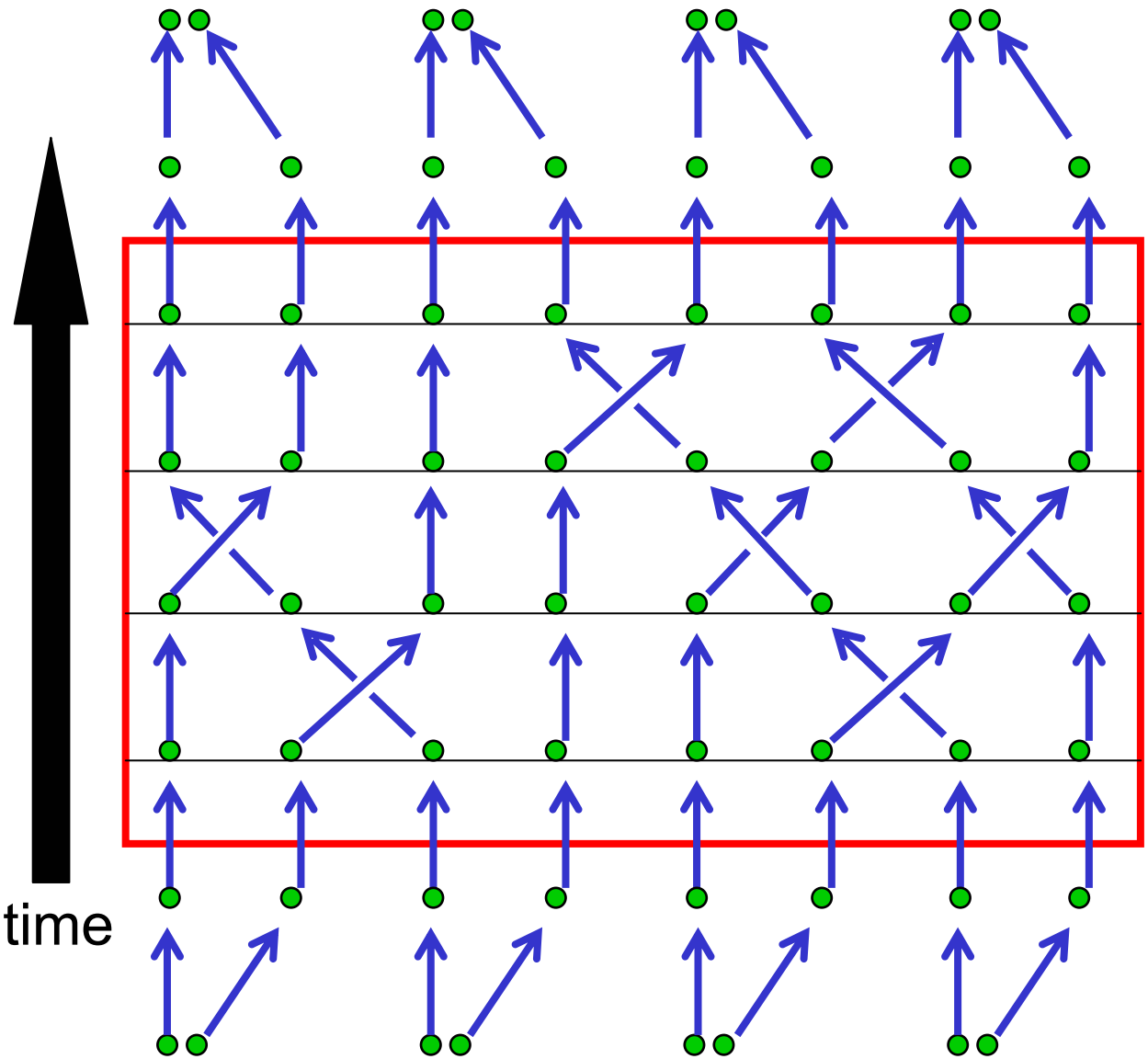
Anyons

Quantum information can be stored in the collective state of exotic particles in two dimensions (“anyons”).



The information can be processed by exchanging the positions of the anyons (even though the anyons never come close to one another).

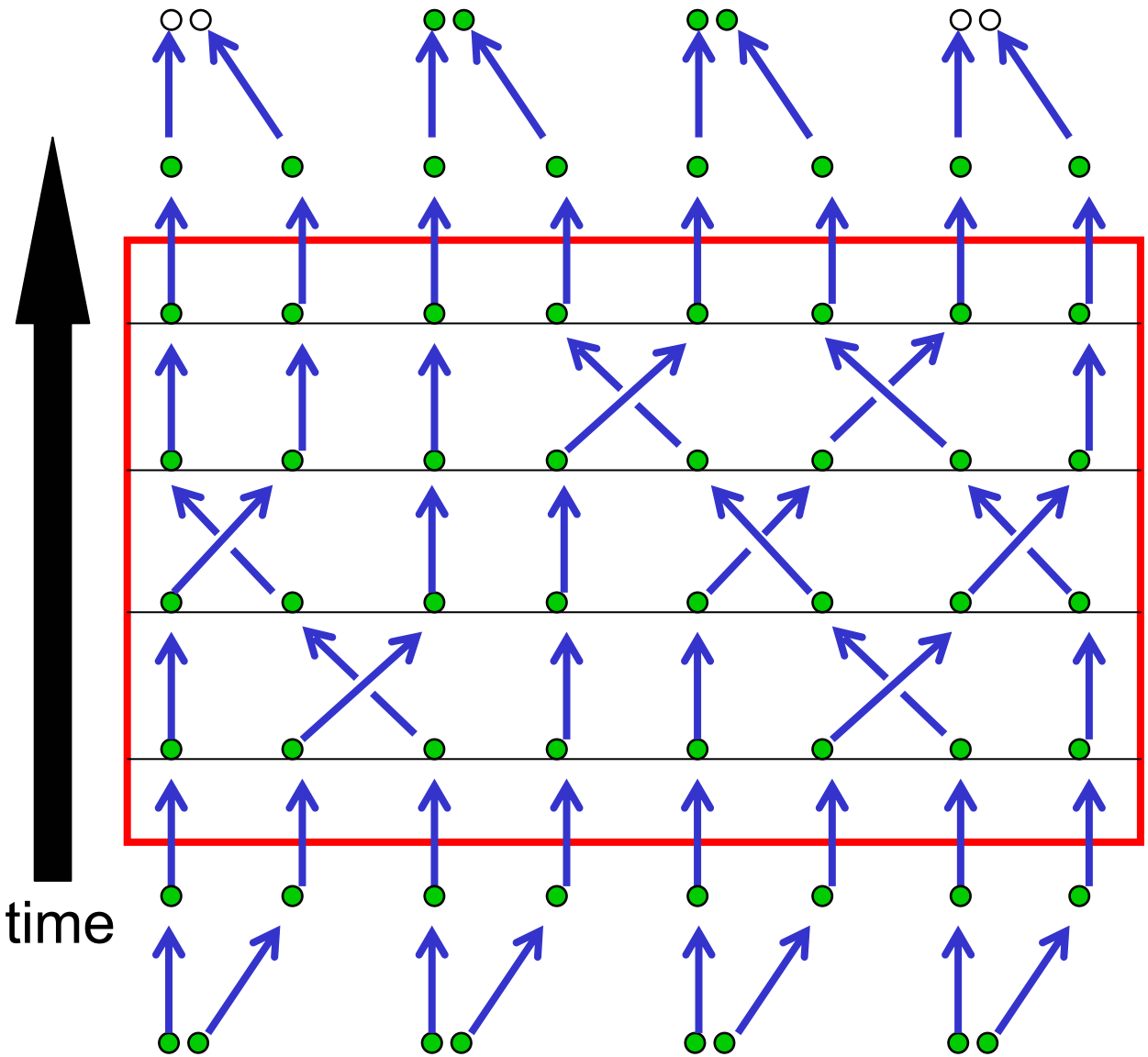
Topological quantum computation (Kitaev '97, FLW '00)



Kitaev

Freedman

Topological quantum computation (Kitaev '97, FLW '00)



annihilate pairs?

braid

braid

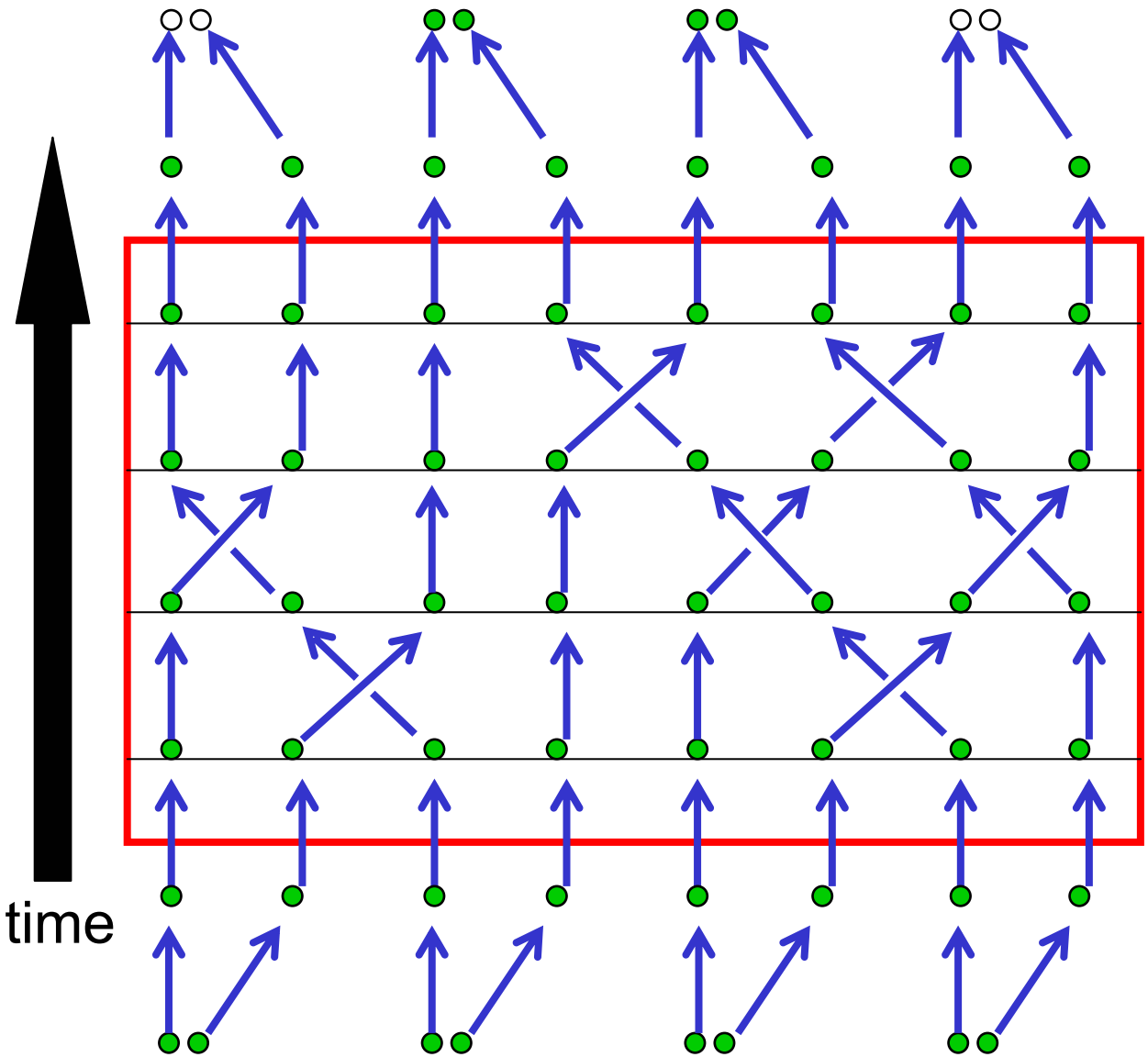
braid

create pairs

Kitaev

Freedman

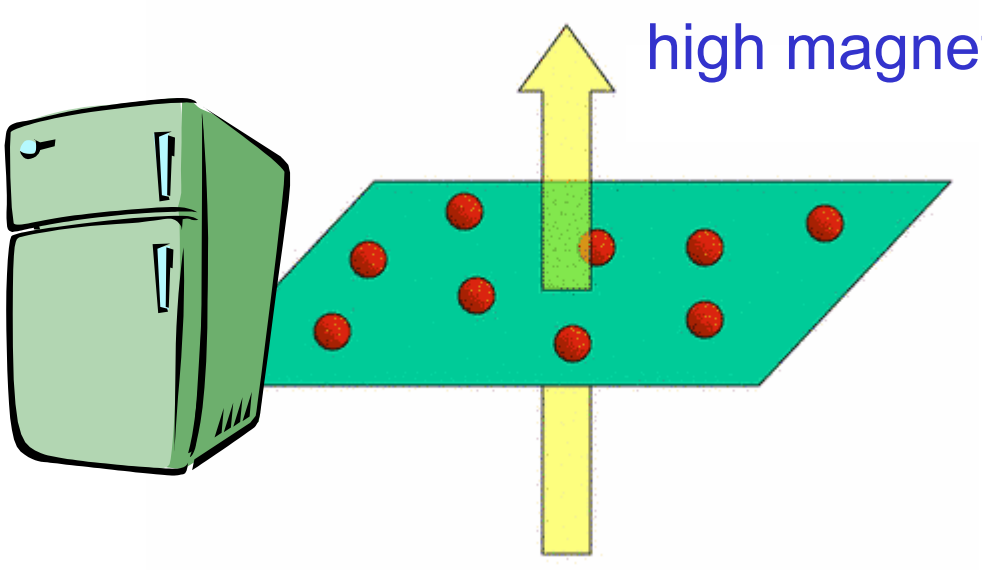
Topological quantum computation



The computation is intrinsically resistant to decoherence.

If the paths followed by the particles in spacetime execute the right braid, then the quantum computation is guaranteed to give the right answer!

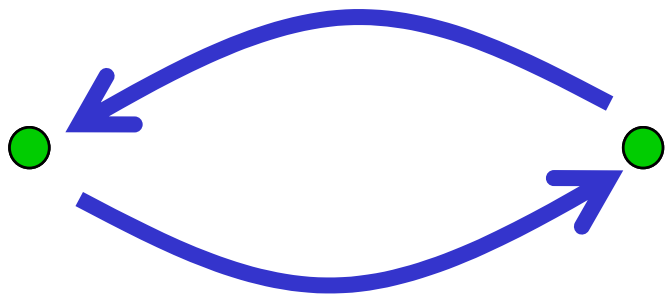
Anyons: the fractional quantum Hall effect

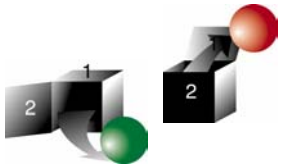


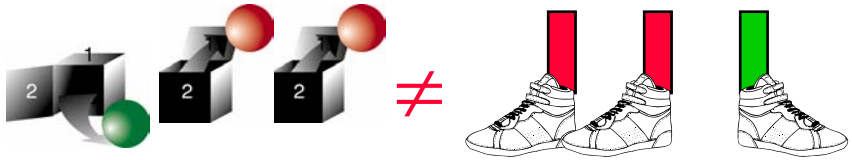
electrons moving freely on a “table,” at very low temperature

An exotic new phase of matter, with particle excitations that are profoundly different than electrons.

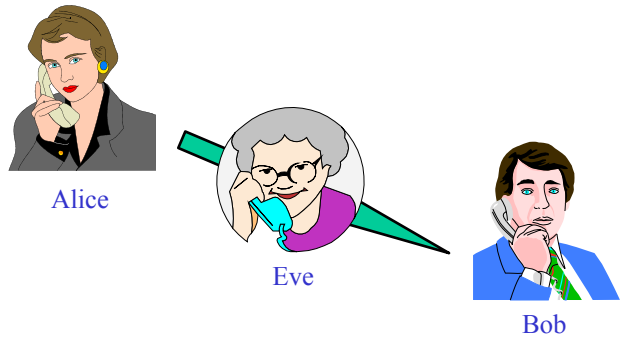
These particles are *anyons*: they have topological interactions.

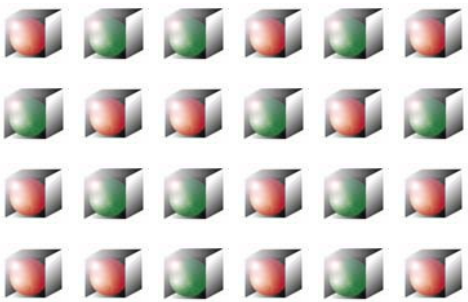


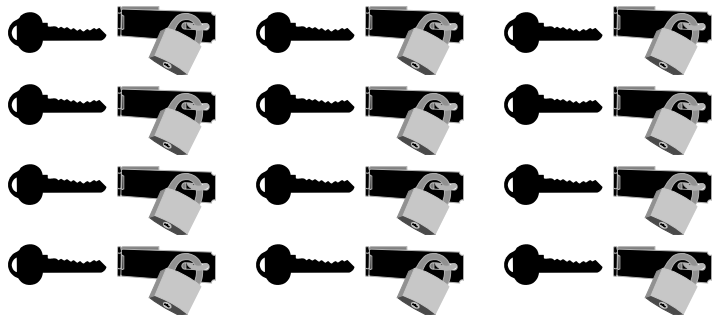


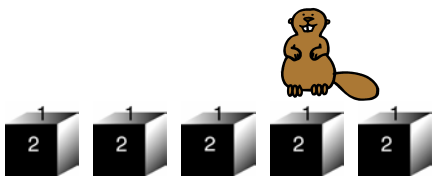


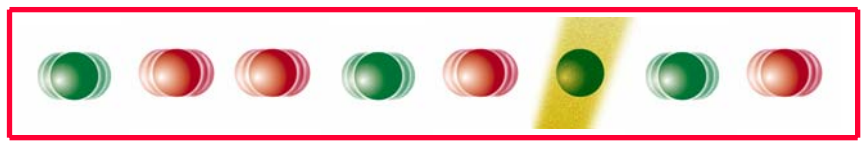

Quantu
Copier


Alice
Eve
Bob



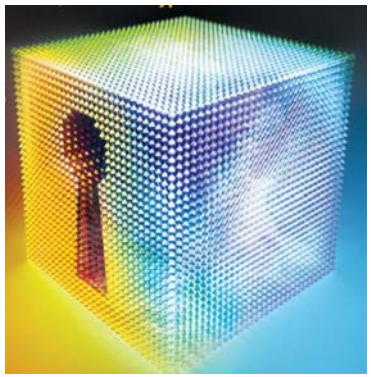






Quantum Information Challenges

Cryptography



Privacy from physical principles

Algorithms

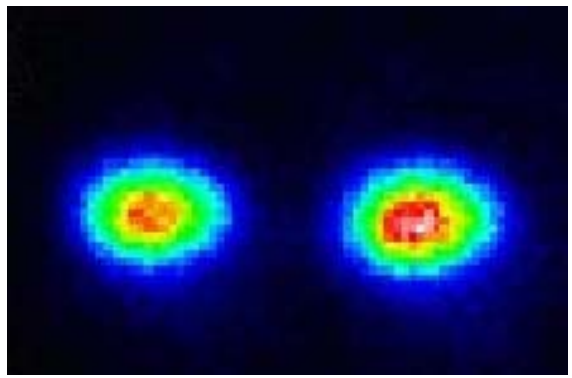
$$\sum_{x \in G} |x\rangle \otimes |f(x)\rangle$$

What can quantum computers do?

Error correction

Reliable quantum computers

Hardware



Toward scalable devices

And …what are the implications of these ideas for basic physics?

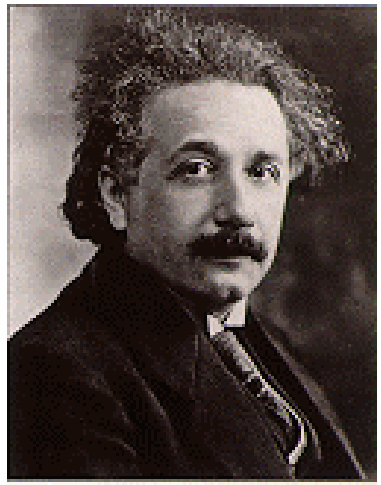
MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

(Received March 25, 1935)

In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system. In quantum mechanics in the case of two physical quantities described by non-commuting operators, the knowledge of one precludes the knowledge of the other. Then either (1) the description of reality given by the wave function in quantum mechanics is not complete or (2) these two quantities cannot have simultaneous reality. Consideration of the problem of making predictions concerning a system on the basis of measurements made on another system that had previously interacted with it leads to the result that if (1) is false then (2) is also false. One is thus led to conclude that the description of reality as given by a wave function is not complete.



Einstein saw, sooner and more clearly than others, the essential weirdness at the core of quantum theory, what Schrödinger called “quantum entanglement.”

To Einstein, this “spooky action at a distance” presaged the emergence of a deeper theory that would supersede quantum mechanics. In the 70 years since 1935, that has not happened.

But EPR’s insight that quantum entanglement signifies an especially profound (*weird*) departure from the classical description of Nature has been amply vindicated. And now we face the exciting challenge of *putting the weirdness to work*.