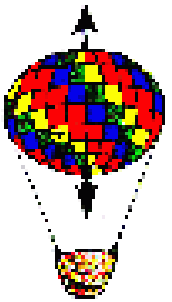
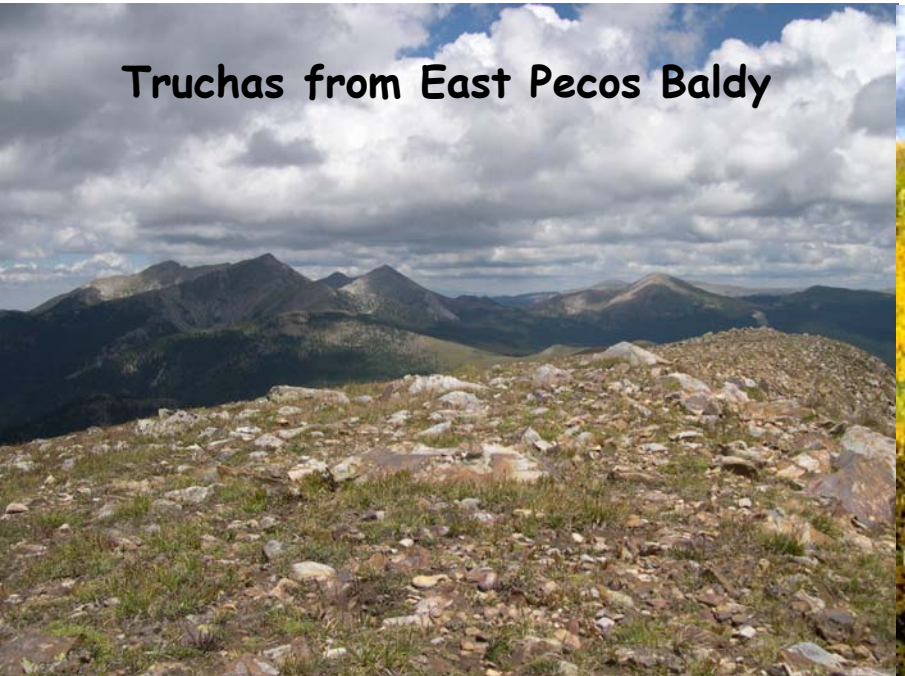
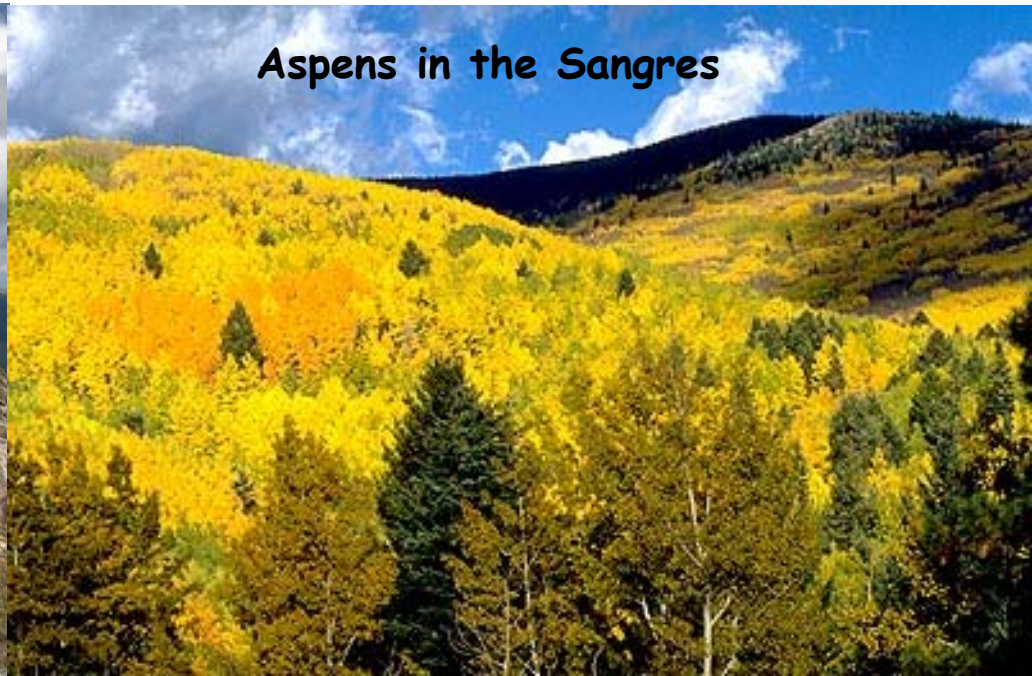
What the #$*! Do We (K)now!? about Quantum Communication

Carlton M. Caves
University of New Mexico
http://info.phys.unm.edu/~caves



CAPS, University of New Mexico
2007 February 23





Quantum communication

Communication using quantum systems

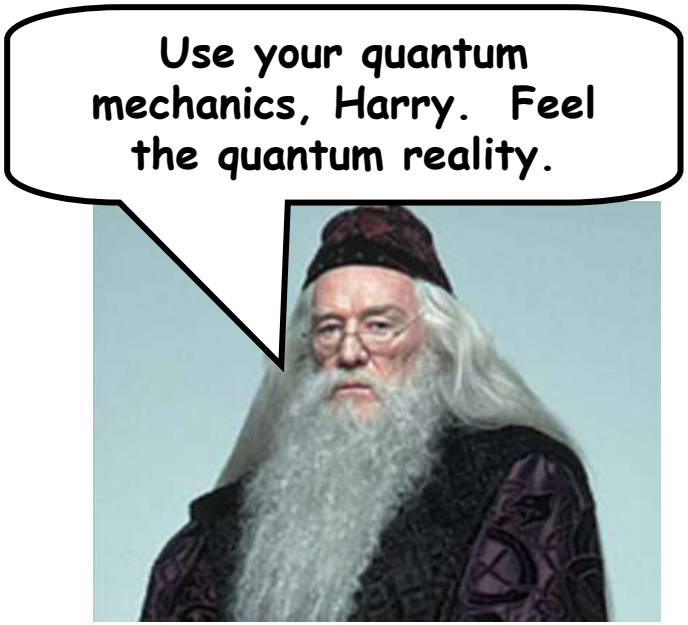
Quantum mechanics as limiter

Using quantum systems to communicate in ways that cannot be done classically

Using quantum systems to perform information-processing tasks that cannot be done classically

Quantum mechanics as enabler

Quantum information science



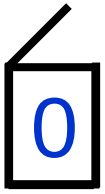
Message

H E L P

00111 00100 01011 01111

Alice

Bob



Message

H E L P

00111 00100 01011 01111

Alice

Bob

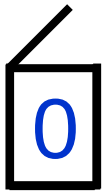
Message

H E L P

00111 00100 01011 01111

Alice

Bob



Eve

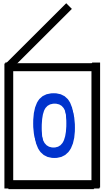
Message

H E L P

00111 00100 01011 01111

Alice

Bob



Eve

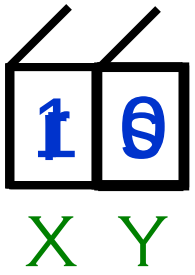
Private communication

Alice and Bob share a one-time pad (secret random key).

	00111001000101101111	Message
$\oplus$	01110010011010010011	Key (random string)
	01001011011111111100	Coded message
$\oplus$	01110010011010010011	Key (random string)
	00111001000101101111	Message

But where do Alice and Bob get the key?

"Two-bit" device



Rules

1. An interlock mechanism permits only one box at a time to be opened.
2. When a box is opened, the interlock also causes a random bit to be placed in the other box.

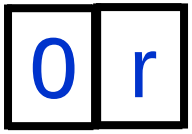
Information capacity = 1 bit

If you try to send 2 bits encoded in which box and what's in that box, you end up sending only half a bit.

Secret key distribution

ALICE

BOB



X

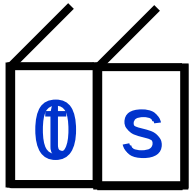
Secret key distribution

ALICE

BOB

0

X

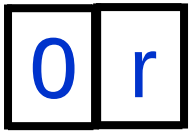


X Y

Secret key distribution

ALICE

BOB



X

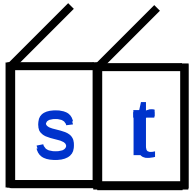
Secret key distribution

ALICE

BOB

0

X



X Y

Secret key distribution

Alice

Bob

1 0 1 0 0 1 0 0 0 1

X X Y X Y Y Y X Y Y

r r r 0 r 1 r 0 0 r

Y Y X X X Y X X Y X

Alice and Bob announce their box sequences publicly and keep the bits only when the boxes agree. This process, called *sifting,* yields a shared secret key, in this case

0100

The key generation rate is 50% (1/2 bit per try).

Alice

1. Alice and Bob's sifted keys have an error rate of 25%. By sacrificing some key bits, they can detect Eve's presence through the error rate.
2. Eve knows 50% of each of their sifted keys.

Bob

1 0 1 0 0 1 0 0 0 1

X X Y X Y Y Y X Y Y

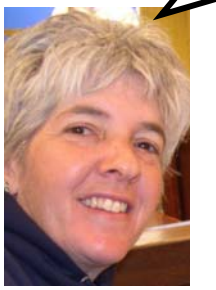
r r r 0 r s r s 0 r

Y Y X X X Y X X Y X

r r r 0 0 r 0

Y Y X X Y X

Heh, heh, heh.



Eve

Error correction and privacy amplification allow Alice and Bob to extract a secret key provided the error rate does not exceed 17.1%.

Flaw: If Eve can deactivate the interlock, she can open both boxes and determine the sifted key without introducing errors.

Secret key distribution

Alice

Quantum mechanics to the rescue!
For quantum systems, the two rules are consequences of the laws of quantum mechanics: there is no hidden interlock mechanism to be de-activated.

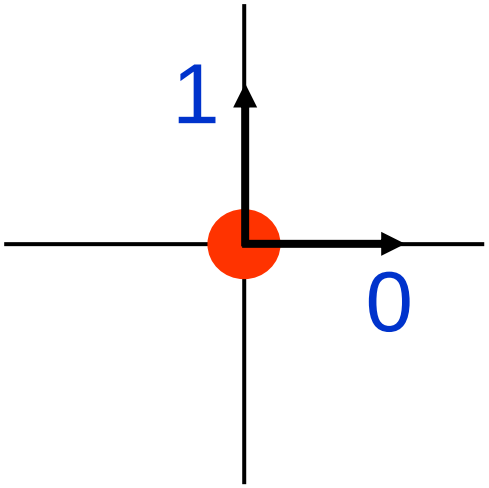
Bob

Eve

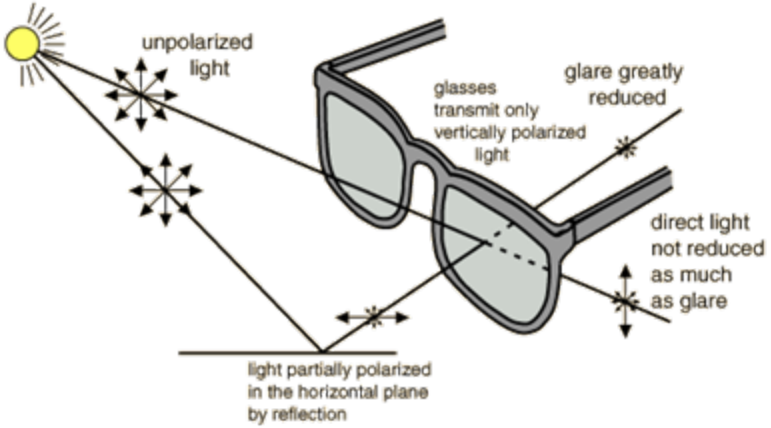
Rats!
Foiled again. I hate those quantum mechanicians.

Qubits: Two-state quantum systems

Photon

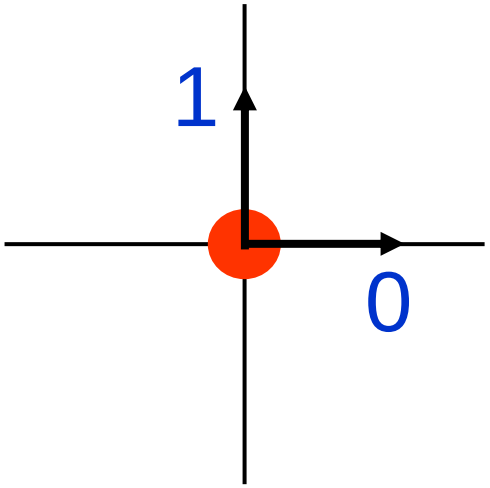


Photon polarization



Qubits: Two-state quantum systems

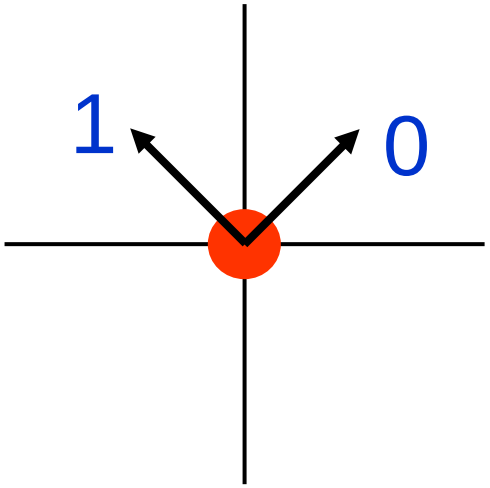
Photon



x

Qubits: Two-state quantum systems

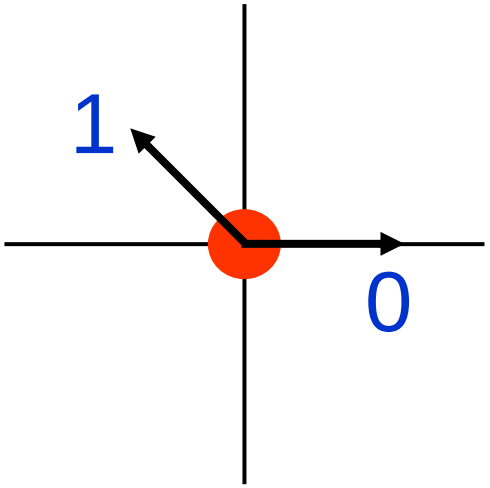
Photon



Y

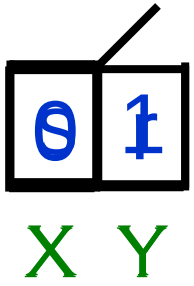
Qubits: Two-state quantum systems

Photon



Quantum rules

1. Only one polarization at a time can be prepared or measured.
2. When one polarization is measured, the other is randomized.

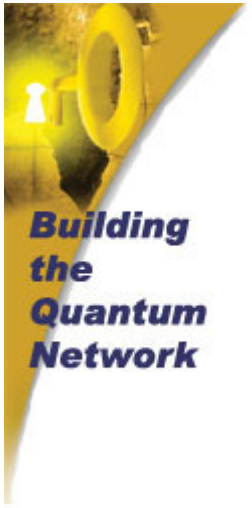


Quantum key distribution in the real world

HTTP://WWW.MAGIQTECH.COM/

Quantum key distribution in the real world

BBN TECHNOLOGIES



The DARPA Quantum Network: World's First Quantum Cryptographic Network

Under DARPA sponsorship, and together with our academic colleagues, Harvard University and Boston University, BBN Technologies has recently built and begun to operate the world's first Quantum Key Distribution (QKD) network. The DARPA Quantum Network employs 24x7 quantum cryptography to provide unprecedented levels of security for standard Internet traffic flows such as web-browsing, e-commerce, and streaming video.

The DARPA Quantum Network became fully operational on October 23, 2003 in BBN's laboratories, and has run continuously since. It currently consists of two BBN-built, interoperable weak-coherent QKD systems running at a 5 MHz pulse rate (0.1 mean photons per pulse) through telecommunications fiber, and inter-connected via a photonic switch, together with a full suite of production-quality QKD protocols. In the near future, we plan to roll out this network into dark fiber between our campuses through the Cambridge, Massachusetts metropolitan area, introduce a series of new quantum cryptographic links based on a variety of physical phenomena, and start testing the resulting network against sophisticated attacks.

http://www.bbn.com/networking/quantumcryptography.html

Quantum key distribution in the real world

LANL Quantum Institute

http://quantum.lanl.gov/

Although the quantum key distribution technique was not created at Los Alamos, laboratory researchers have taken the technology, quite literally to new lengths in the interest of national security. In 1999, Los Alamos researchers set a world record when they sent a quantum key through a 31-mile-long optical fiber. ... Los Alamos researchers developed a free-space quantum cryptography system that could send keys through the air.

Los Alamos quantum scientists developed a transportable, self-contained QKD system that used polarized photons to send information through the air for distances of up to 10 miles. This mobile trailer-based QKD system could be quickly deployed in the field and was capable of continuous, automated transmission in both daylight and darkness. Today, Los Alamos researchers are in the process of taking this technology even further by developing a smaller scale version that is capable of being put on an Earth-orbiting satellite for transmitting quantum keys distances of hundreds of miles between the satellite and a ground station.

What happened to Planck's constant?

Max Planck (1858-1947)

Planck initiated the study of quantum mechanics when he announced in 1900 the results of his theoretical research into the radiation and absorption of a "black body."

$$h = 6.6261 \times 10^{-34} \text{ Joule-sec}$$

Planck's constant is the scale on which physical phenomena are discrete (or grainy); for example, photons are the expression of the discreteness of the electromagnetic field.

World of classical physics

World of quantum physics

Continuous, smooth (analogue)

I don't care if you are at Hogwarts, Harry. You can't violate the uncertainty principle.

Discrete, grainy (digital)

Information-processing perspective

Use your quantum mechanics, Harry. Feel the quantum reality.

Digital devices (on-off)

Continuum of on-off properties

Classical bit vs. quantum bit

A classical bit is either on or off.

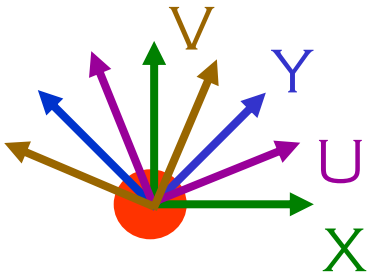
- A few electrons on a capacitor
- A pit on a compact disk
- A 0 or 1 on the printed page
- A smoke signal rising from a distant mesa

A quantum bit (qubit) has a continuum of on-off properties.

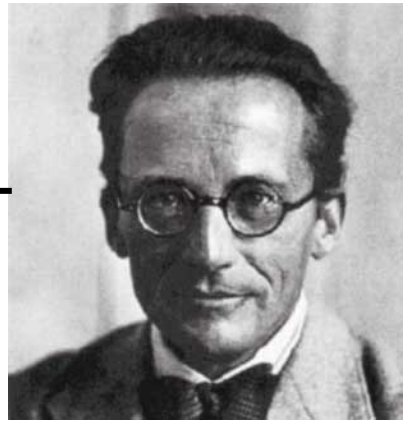
on-off

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

continuum



CONTINUUM OF ONE-BIT BOXES



ERWIN SCHRÖDINGER (1881-1961)

NIELS BOHR (1885-1962)

World of classical physics **World of quantum physics**

Continuous, smooth (analogue)

I don't care if you are at Hogwarts, Harry. You can't violate the uncertainty principle.

Discrete, grainy (digital)

Information-processing perspective

Use your quantum mechanics, Harry. Feel the quantum reality.

Digital devices (on-off)

Continuum of on-off properties

Combination of analogue and digital: analogue information processing made digital by measurements.

Why is quantum key distribution secure?

An unopened box has no bit value waiting to be discovered.

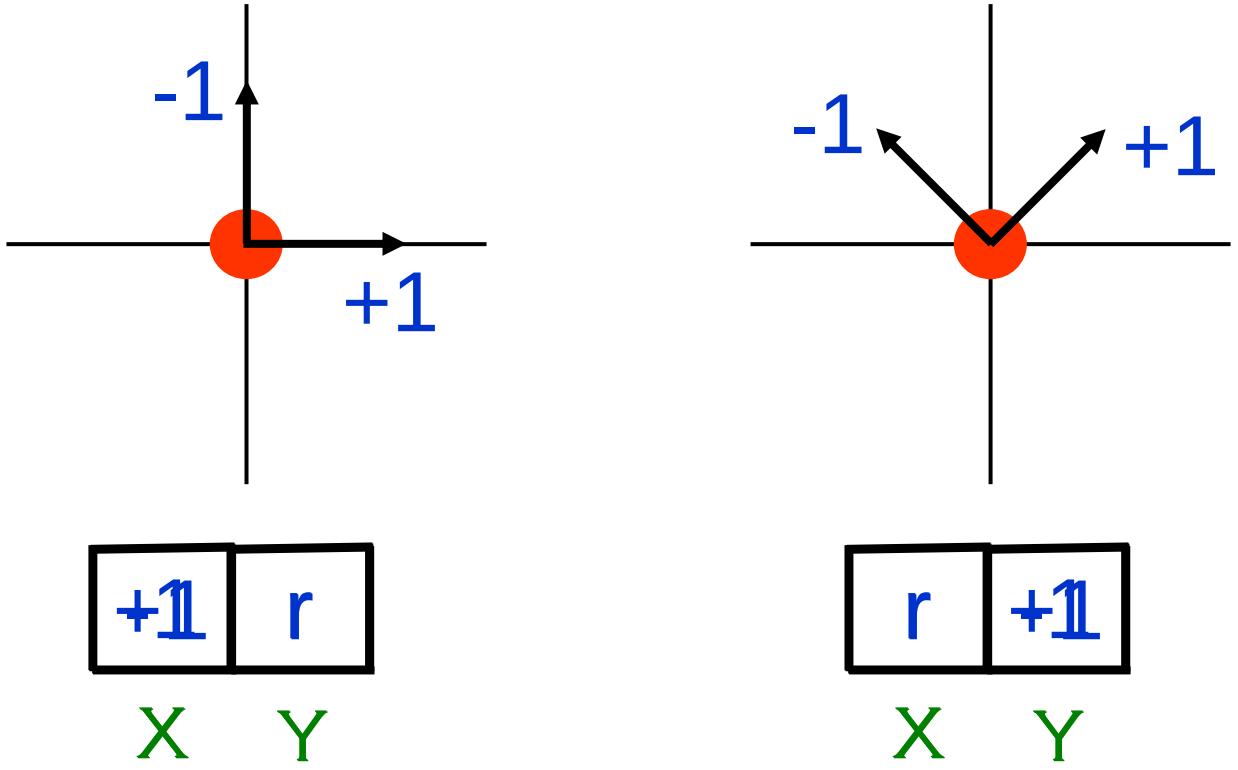
Entanglement between qubits

Albert Einstein (1879-1955)

John S. Bell (1928-1990)

N. David Mermin (1935-)

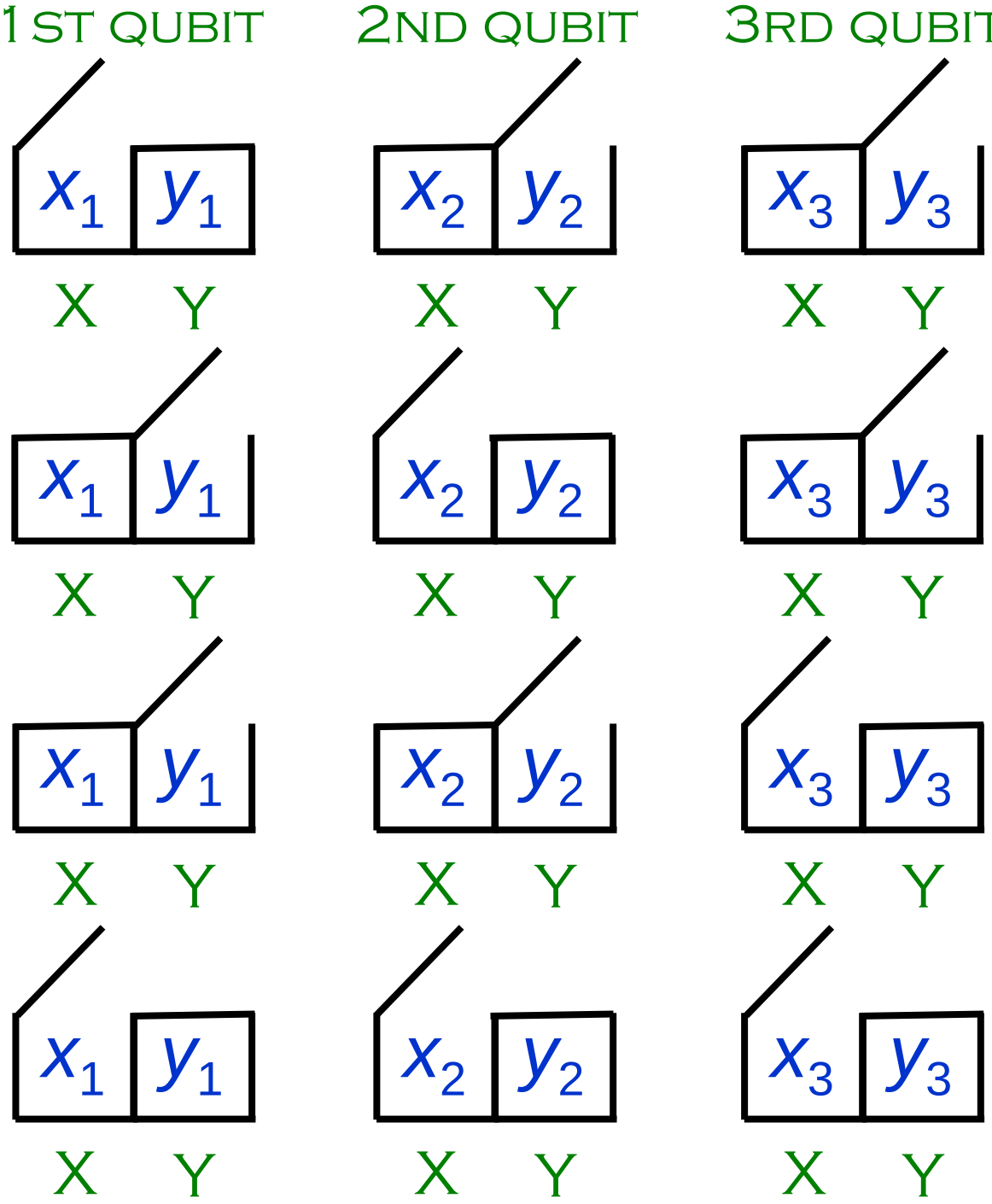
Qubits: Two-state quantum systems

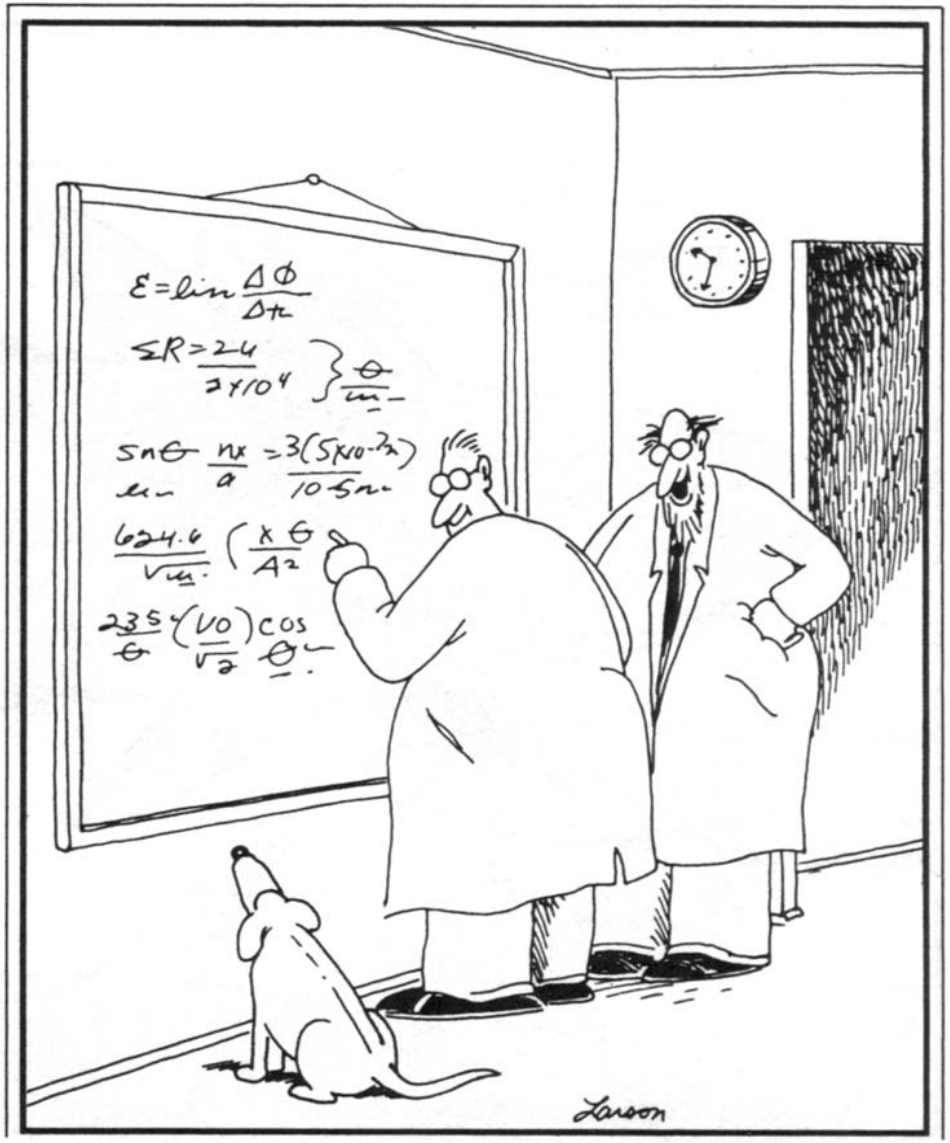


Greenberger-Horne-Zeilinger (GHZ) entanglement

3-QUBIT GHZ ENTANGLED STATE: $|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$

1ST QUBIT	2ND QUBIT	3RD QUBIT
x_1 y_1	x_2 y_2	x_3 y_3
X Y	X Y	X Y


1ST QUBIT
2ND QUBIT
3RD QUBIT
x_1 y_1
x_2 y_2
x_3 y_3
X Y
$x_1 y_2 y_3 = -1$
$y_1 x_2 y_3 = -1$
$y_1 y_2 x_3 = -1$
$x_1 x_2 x_3 = ?\text{-}1$
QM: $x_1 x_2 x_3 = +1$



"Ohhhhhh…Look at that, Schuster…Dogs are so cute when they try to comprehend quantum mechanics."

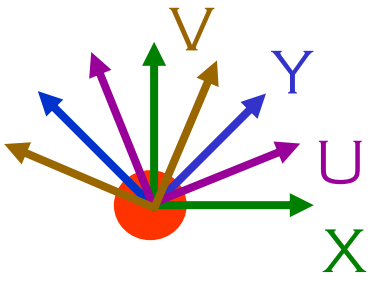
We've shown now that it's not only dogs that can't understand quantum mechanics, so …

Quantum information science is the discipline that explores information processing within the quantum context where the mundane constraints of realism and determinism no longer apply.

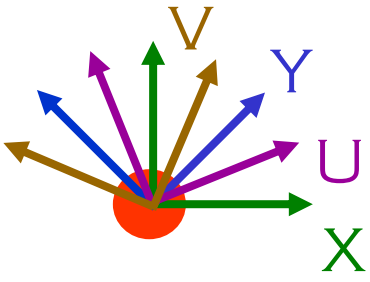
Quantum key distribution using entanglement

2-QUBIT BELL ENTANGLED STATE: $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

1ST QUBIT



2ND QUBIT



x_1	u_1	y_1	v_1
X	U	Y	V

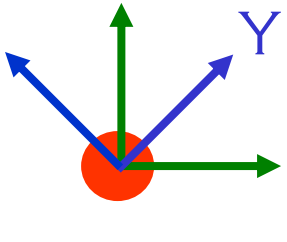
x_2	u_2	y_2	v_2
X	U	Y	V

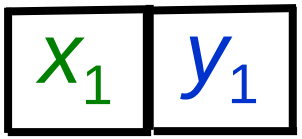
Bell correlations

$$x_1x_2 = u_1u_2 = y_1y_2 = v_1v_2 = -1$$

A Bell inequality

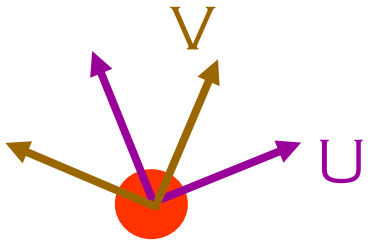
1ST QUBIT

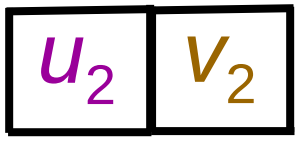




X Y

2ND QUBIT





U V

2ND QUBIT

1ST QUBIT

	U	V
X	x_1u_2	x_1v_2
Y	y_1u_2	y_1v_2

$$S = x_1u_2 + y_1u_2 + y_1v_2 - x_1v_2$$

$$S = x_1(u_2 - v_2) + y_1(u_2 + v_2) = \pm 2$$

AVERAGE OF S

$$-2 \leq \overline{S} \leq 2$$

QM: $S = 2\sqrt{2} = 2.828$

Quantum key distribution using entanglement

2-QUBIT BELL ENTANGLED STATE:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

1ST QUBIT

x_1	u_1	y_1	v_1
X	U	Y	V

2ND QUBIT

x_2	u_2	y_2	v_2
X	U	Y	V

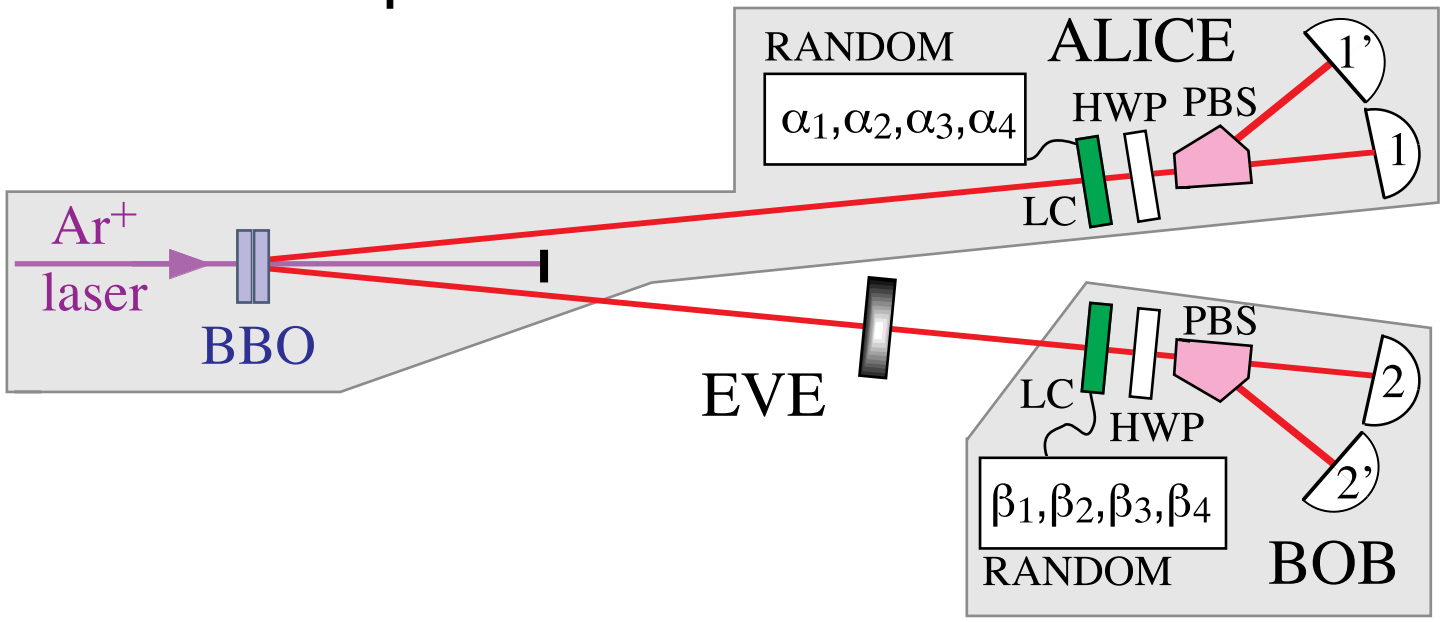
2ND QUBIT

1ST QUBIT	X	U	Y	V
X	$x_1x_2 = -1$ Key	x_1u_2 S	x_1y_2 -	x_1v_2 S
U	u_1x_2 S'	$u_1u_2 = -1$ Key	u_1y_2 S'	u_1v_2 -
Y	y_1x_2 -	y_1u_2 S	$y_1y_2 = -1$ Key	y_1v_2 S
V	v_1x_2 S'	v_1u_2 -	v_1y_2 S'	$v_1v_2 = -1$ Key

Quantum key distribution using entanglement

Theory: Ekert, PRL **67**, 661 (1991)
Experiment: Naik *et al.*, PRL **84**, 4733 (2000)
Tittel *et al.*, PRL **84**, 4737 (2000)
Jennewein *et al.*, PRL **84**, 4729 (2000)

LANL experiment



Why is quantum key distribution secure?

An unopened box has no bit value waiting to be discovered. Alice and Bob create the key by opening their boxes. Before that, there is no key for Eve to steal.

"There is no there there."
Gertrude Stein damning her native Oakland and inadvertently describing quantum systems.

Essential ingredient: Entanglement between qubits

This photo shows Jeremy Caves walking faster than the shutter speed somewhere in Australia.

Where is it?

Echidna Gorge
Bungle Bungle Range
Purnululu NP
Western Australia

2004 June 28