Introducción a la información cuántica

Juan José García Ripoll

Instituto de Física Fundamental

CSIC
Consejo Superior de Investigaciones Científicas

CSID

CSI:C

www.csic.es


GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN
CSIC
español | català | galego | euskara |
prensa intranet
sobre el csic
actualidad
investigación
ciencia y sociedad
fuentes documentales
formación y empleo
transferencia de conocimiento
Consejo Superio
de Investigacion
Científicas
PERFIL DEL CONTRATANTE »
SEDE ELECTRÓNICA »
PLAN DE ACTUACIÓN
La estategia de la institución de 2010 a 2013
EJES ESTRATÉGICOS
Investigación transdisciplinar orientada a problem
CONCLUYE LA VUELTA AL MUNDO DE MALASPINA
La expedición ha recogido 120.000 muestras que dejan un valioso legado a la comunidad científica

CSIC
Consejo Superior de Investigaciones Científicas

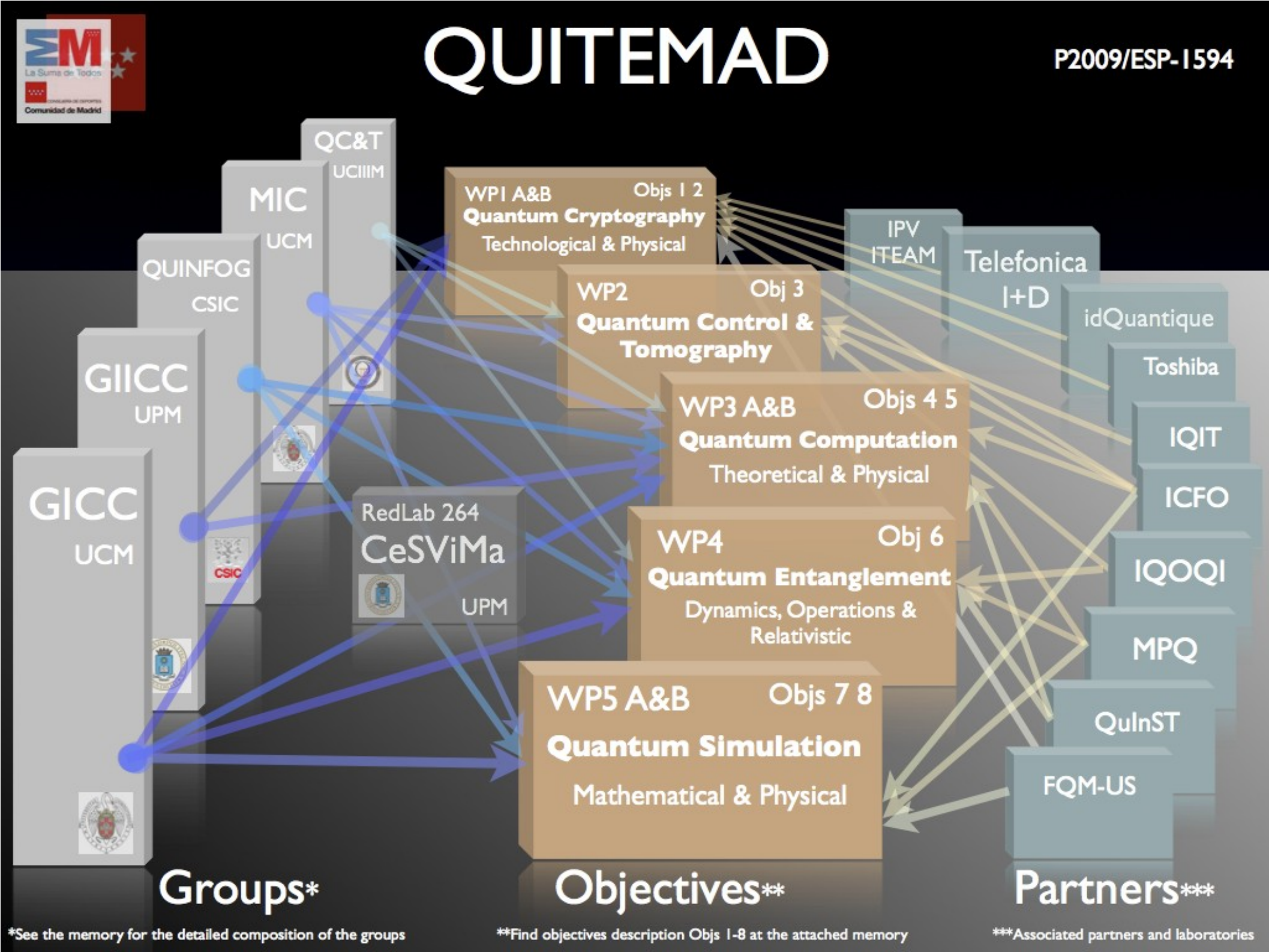
IFF Instituto de Física Fundamental

Quinfog | Miembros | Actividades | Publicaciones | Investigación

http://quinfog.iff.csic.es

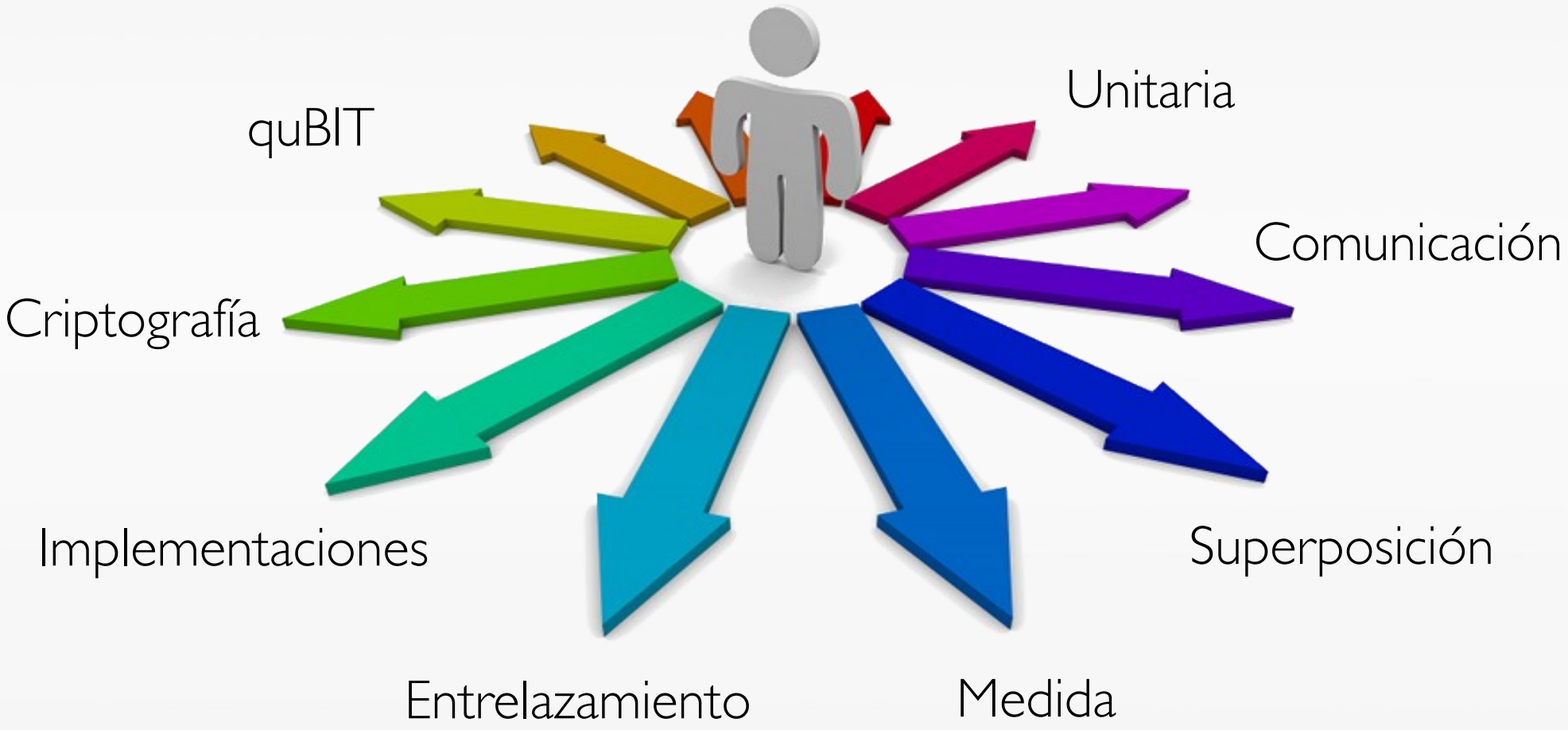
Brewing the best quantum information since 2005...

Tres investigadores de plantilla,
6 doctorandos, 1 postdoc Marie Curie


QUITEMAD
P2009/ESP-1594
QC&T
UCIIIM
MIC
UCM
QUINFOG
CSIC
GIICC
UPM
GICC
UCM
RedLab 264
CeSViMa
UPM
WP1 A&B
Objs 1 2
Quantum Cryptography
Technological & Physical
WP2
Obj 3
Quantum Control & Tomography
WP3 A&B
Objs 4 5
Quantum Computation
Theoretical & Physical
WP4
Obj 6
Quantum Entanglement
Dynamics, Operations & Relativistic
WP5 A&B
Objs 7 8
Quantum Simulation
Mathematical & Physical
IPV
ITEAM
Telefonica I+D
idQuantique
Toshiba
IQIT
ICFO
IQOQI
MPQ
QuInST
FQM-US
Groups*
Objectives**
Partners***
*See the memory for the detailed composition of the groups
**Find objectives description Objs 1-8 at the attached memory
***Associated partners and laboratories

www.quantiki.org

IDEAS


quBIT
Unitaria
Criptografía
Comunicación
Implementaciones
Superposición
Entrelazamiento
Medida

ESQUEMA

Información

Criptografía

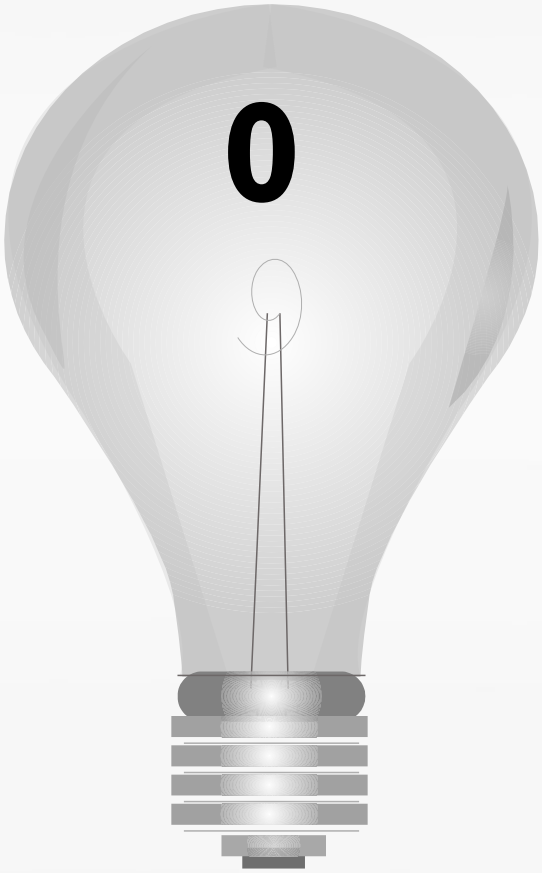
Computación Cuántica

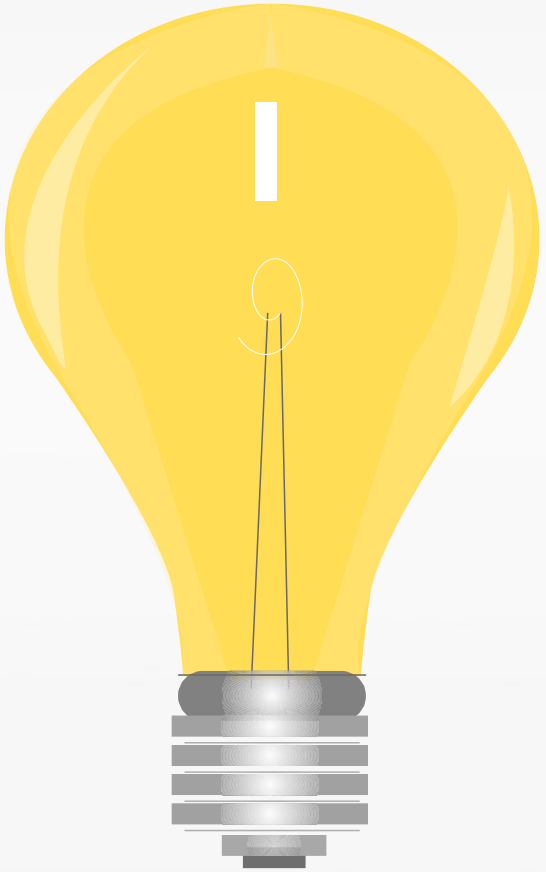
Implementaciones

Circuitos cuánticos

INFORMACIÓN

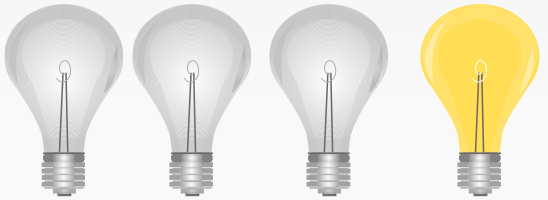
INFORMACIÓN



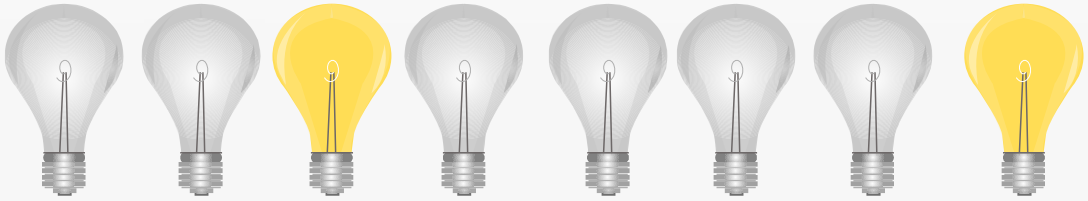


INFORMACIÓN

 = "4"

 = "I"

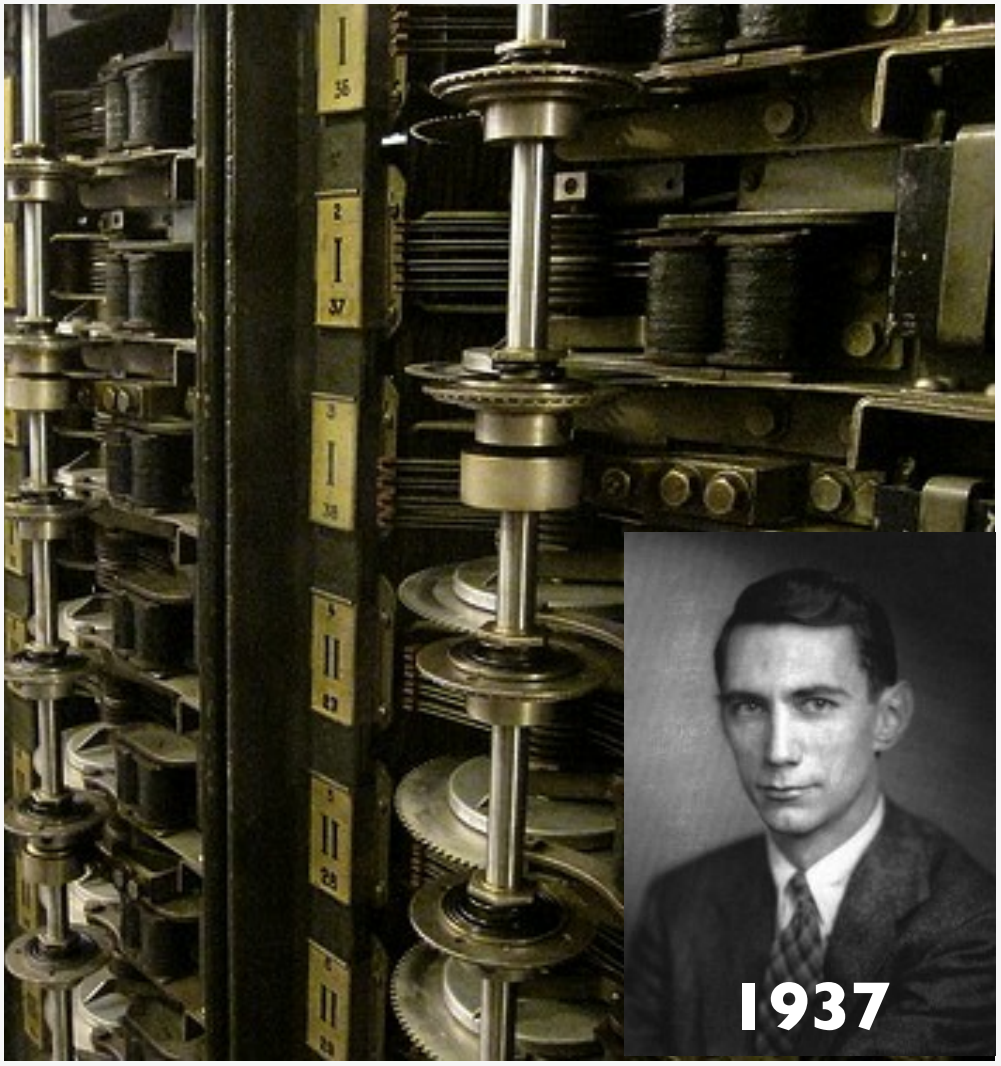
 = "EOT"

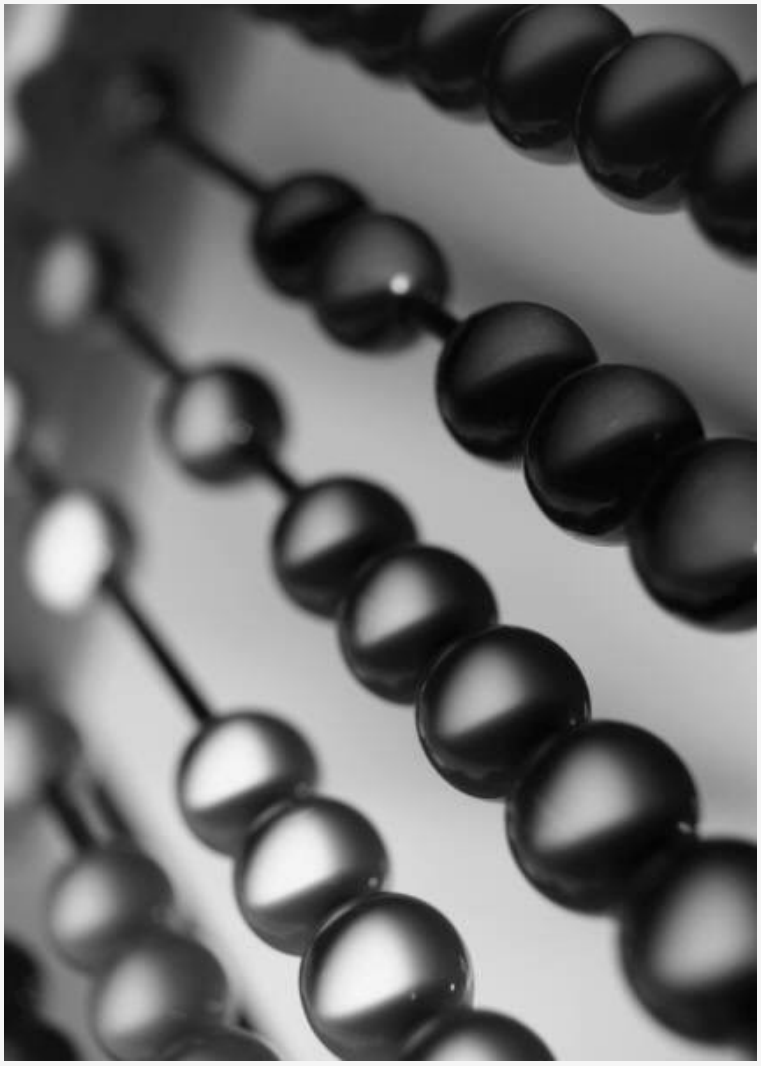
 = "A"

INFORMACIÓN & FÍSICA

- La información es el soporte y sus estados.
- El soporte es físico.
- La información es física
- La física es información.

COMPUTACIÓN

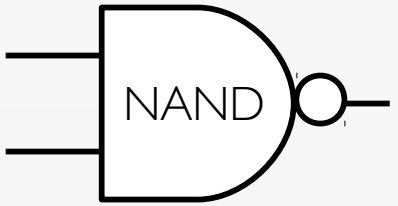




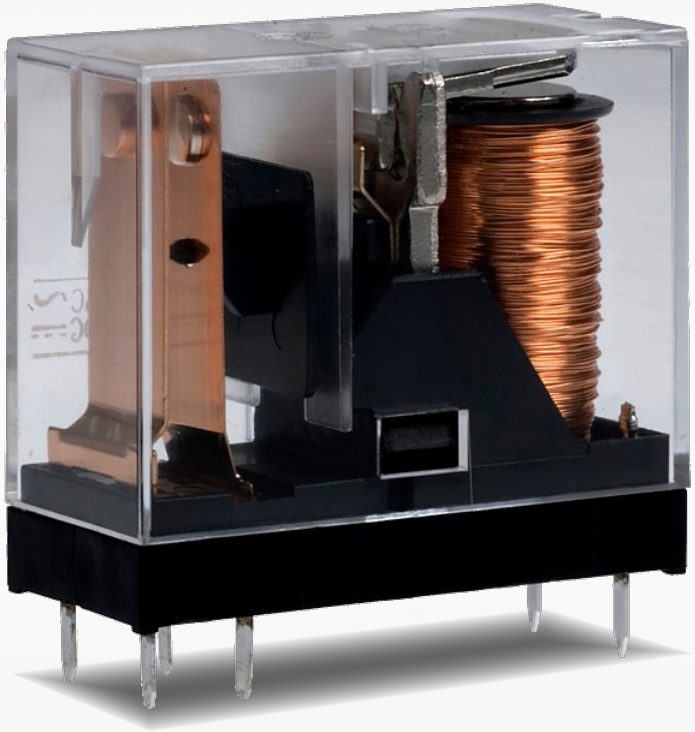
COMPUTACIÓN

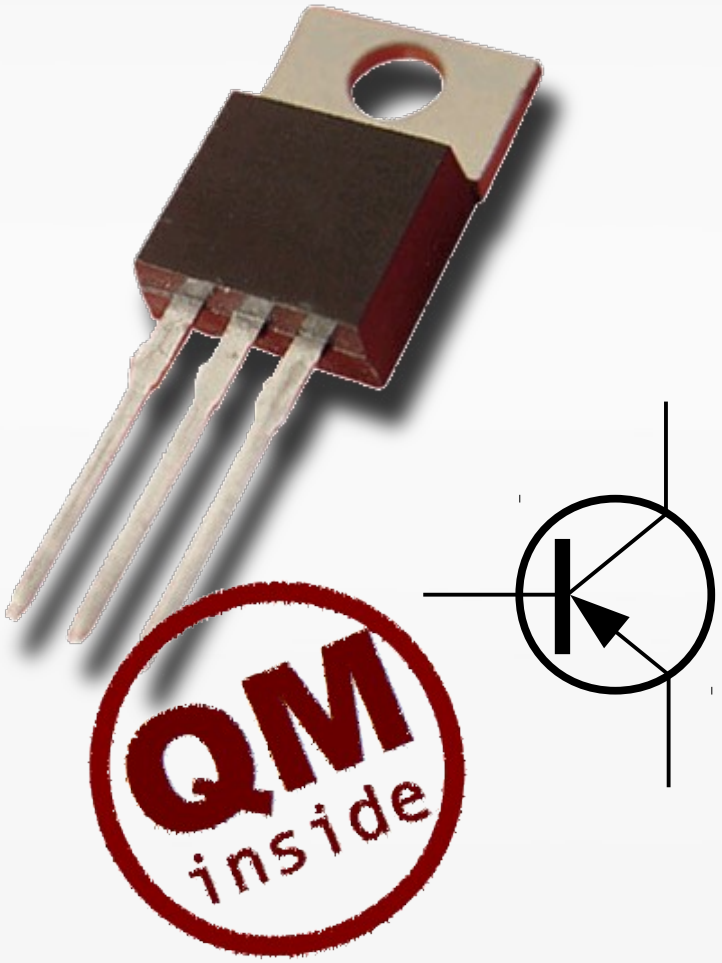
- Elemento de computación básico, puerta NAND

A	B	C
0	0	1
0	1	1
1	0	1
1	1	0

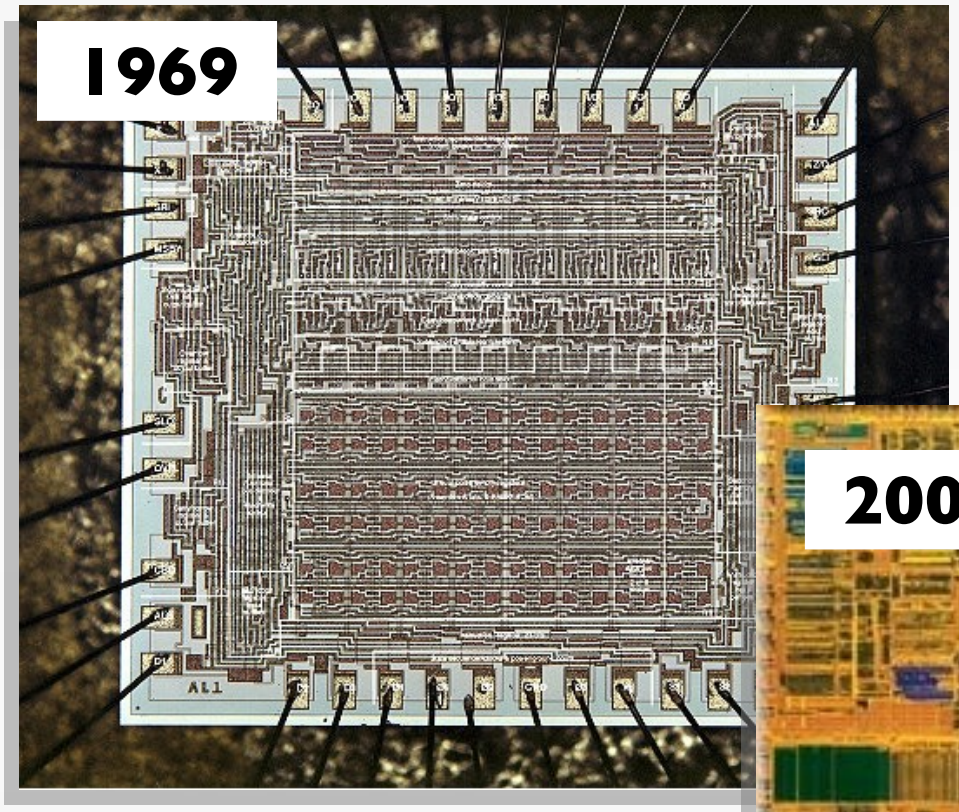


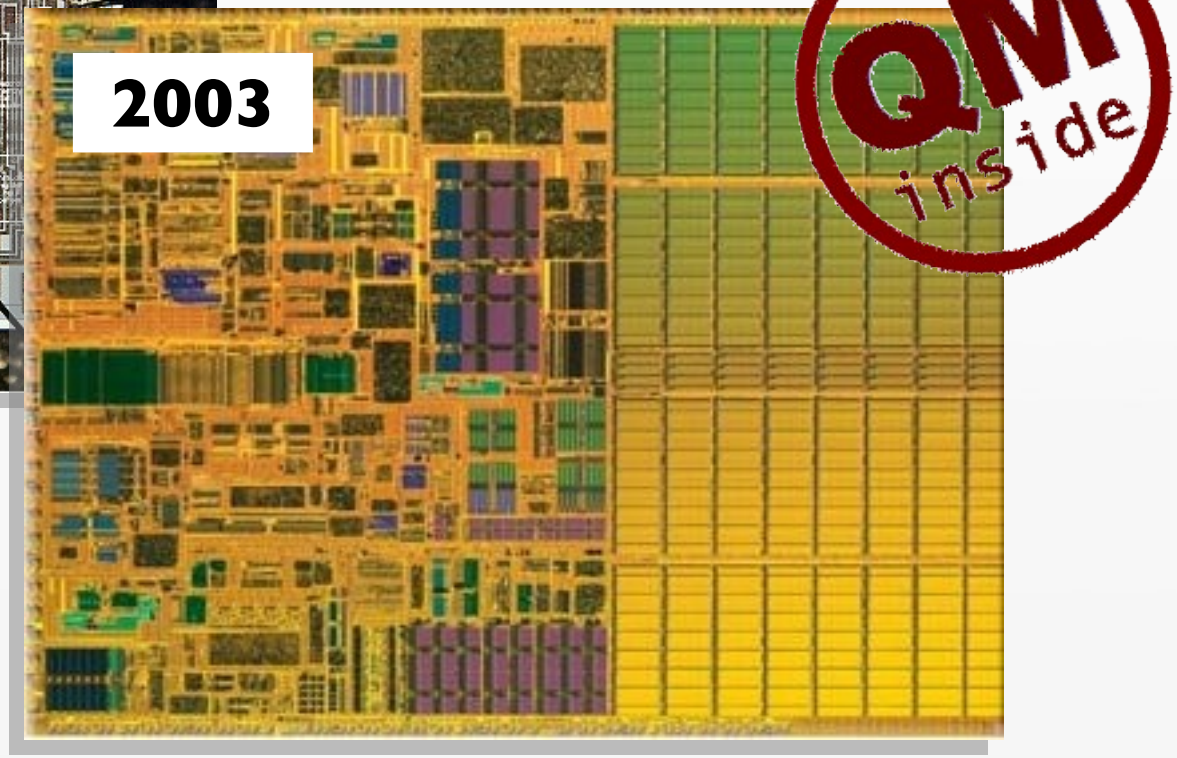
TRANSISTOR



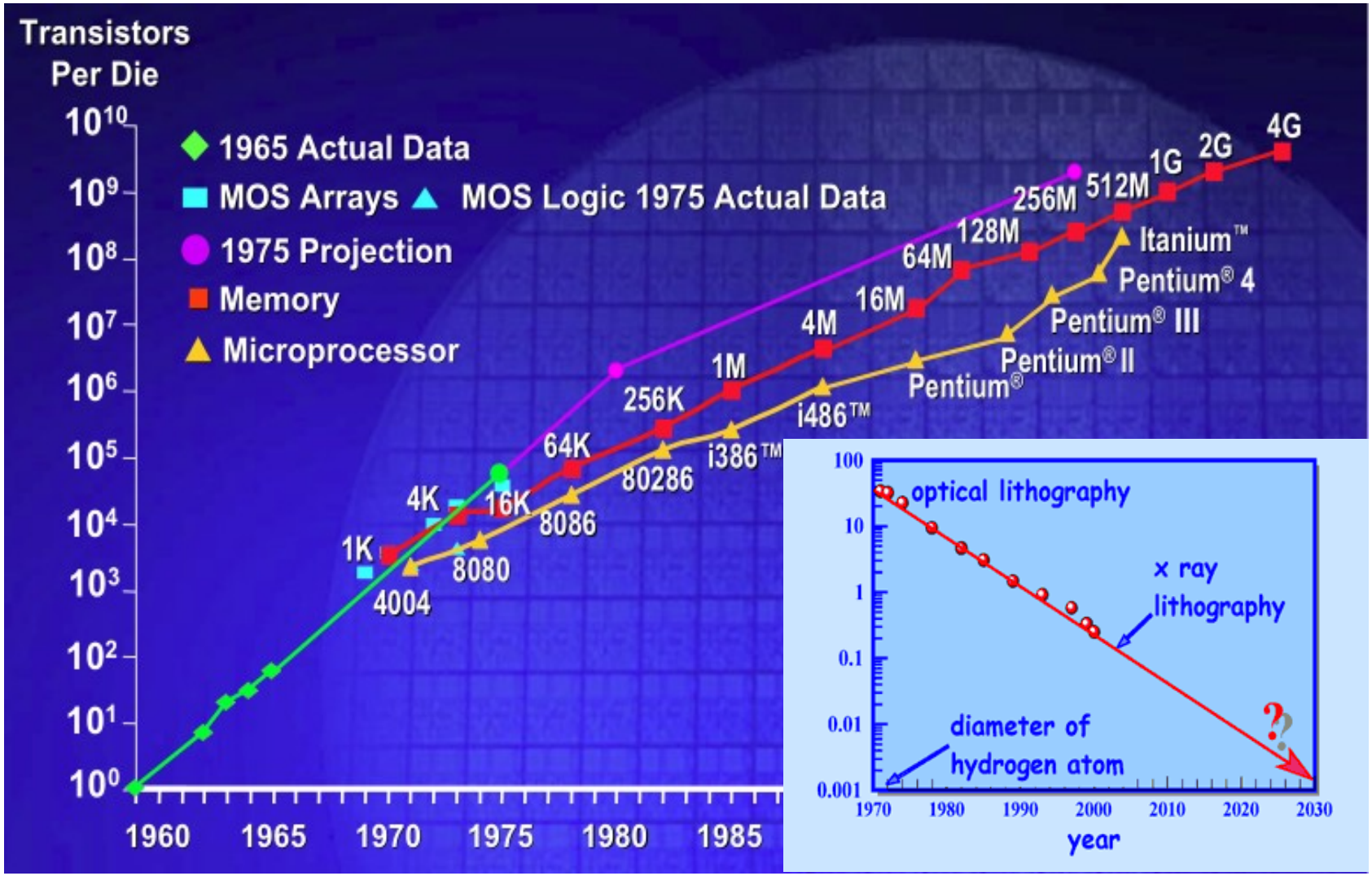


CIRCUITOS INTEGRADOS

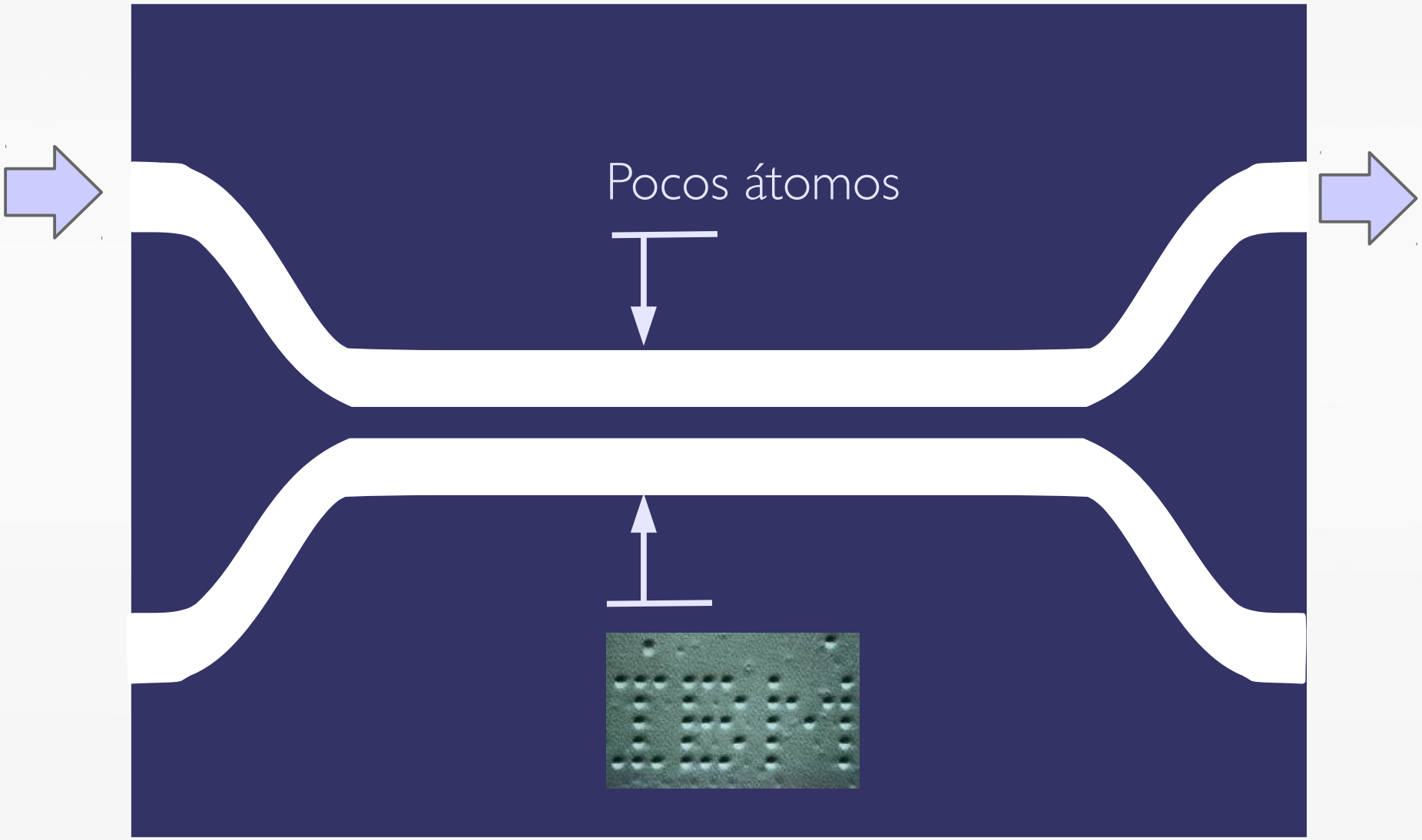




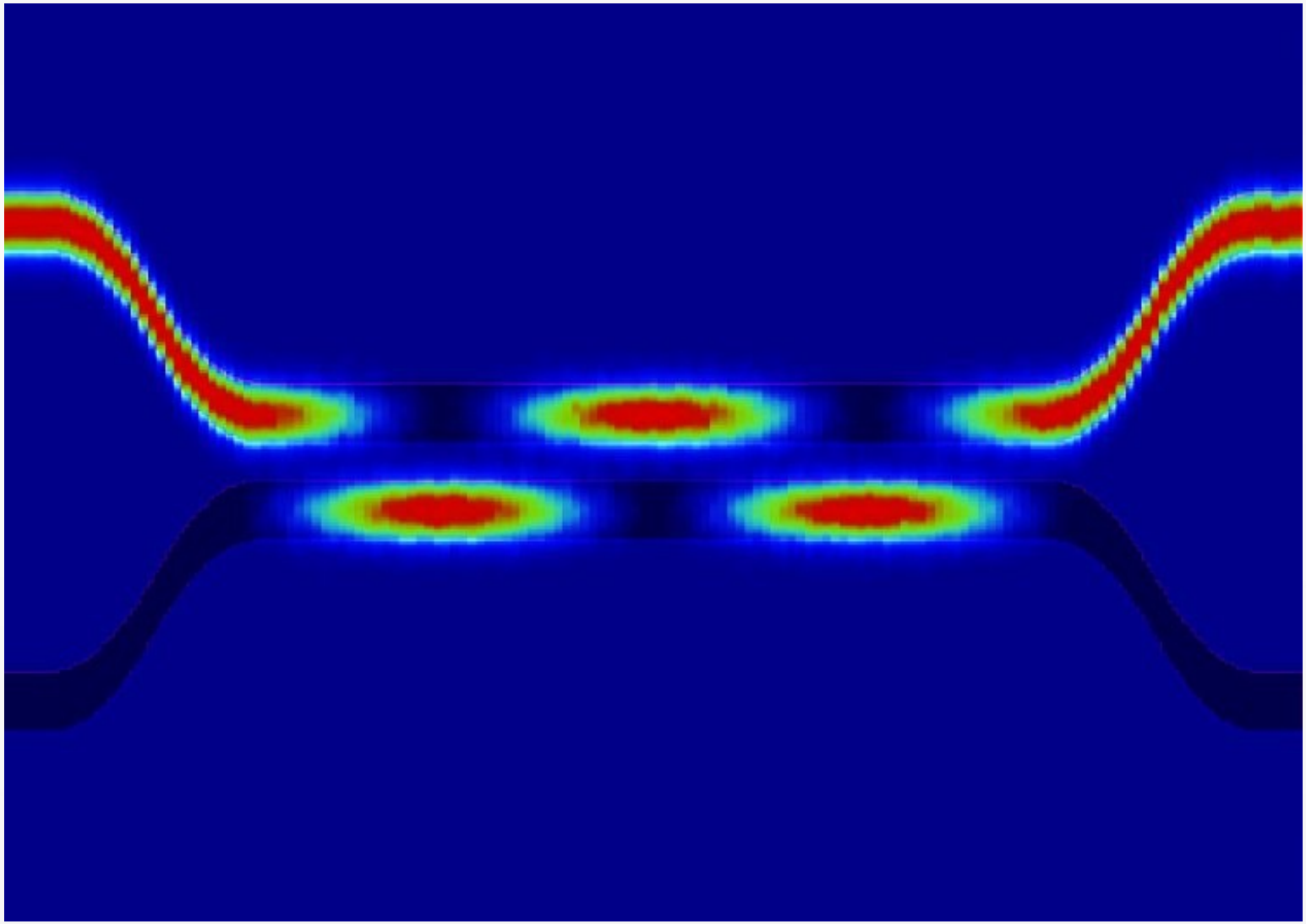
LEY DE MOORE


Transistors
Per Die
10^{10}
10^{9}
10^{8}
10^{7}
10^{6}
10^{5}
10^{4}
10^{3}
10^{2}
10^{1}
10^{0}
1965 Actual Data
MOS Arrays
MOS Logic 1975 Actual Data
1975 Projection
Memory
Microprocessor
1K
4K
16K
64K
256K
1M
4M
16M
64M
128M
256M
512M
1G
2G
4G
4004
8080
8086
80286
i386™
i486™
Pentium®
Pentium® II
Pentium® III
Pentium® 4
Itanium™
1960
1965
1970
1975
1980
1985
100
10
1
0.1
0.01
0.001
optical lithography
x ray
lithography
diameter of
hydrogen atom
?
1970
1980
1990
2000
2010
2020
2030
year

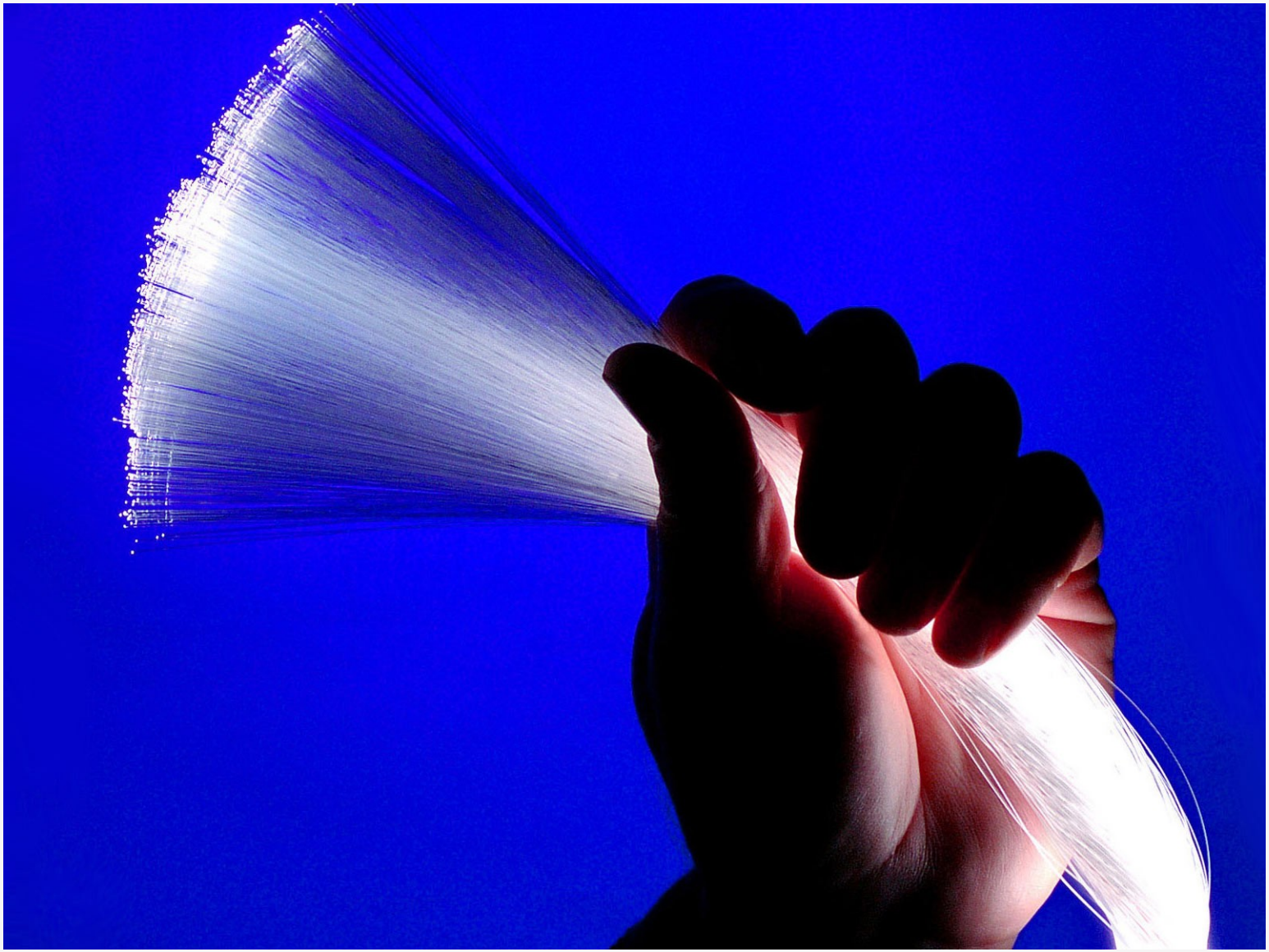
NANOCIRCUITOS



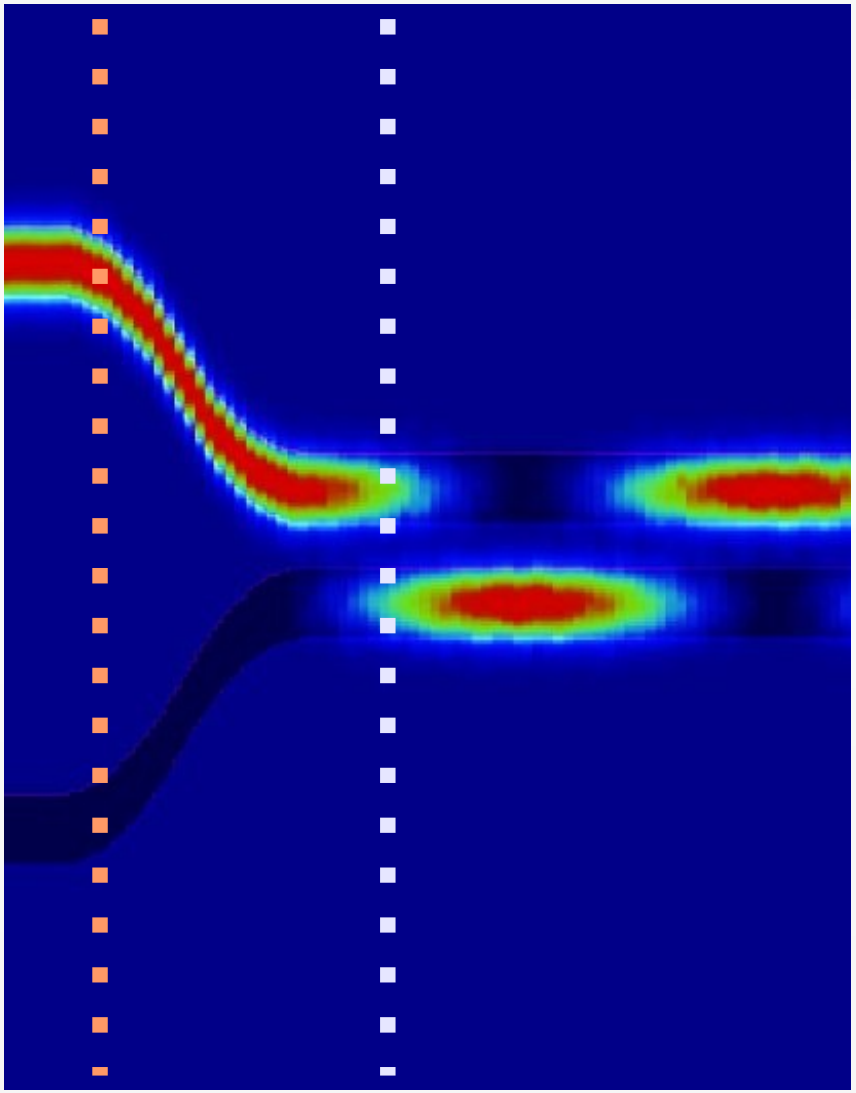
TUNEL CUÁNTICO

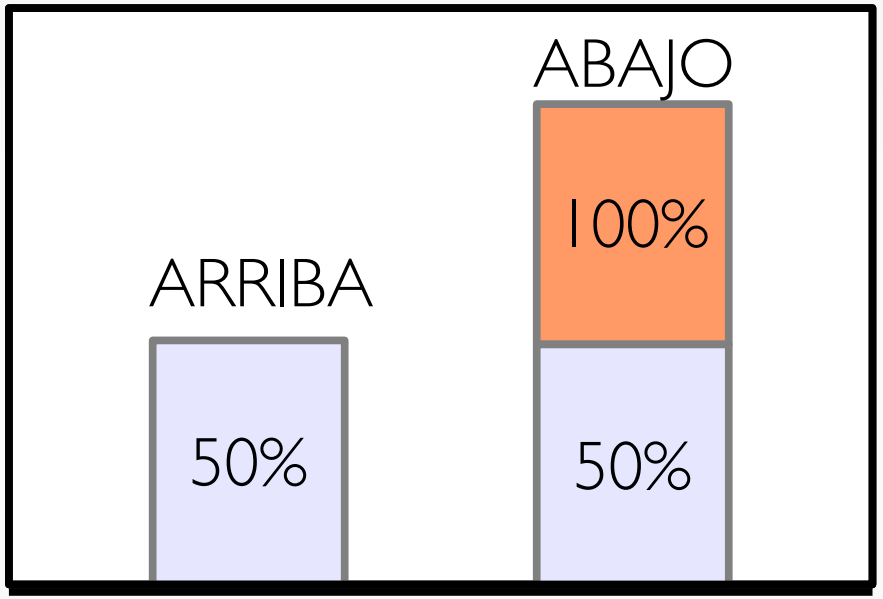


ONDAS



INCERTIDUMBRE

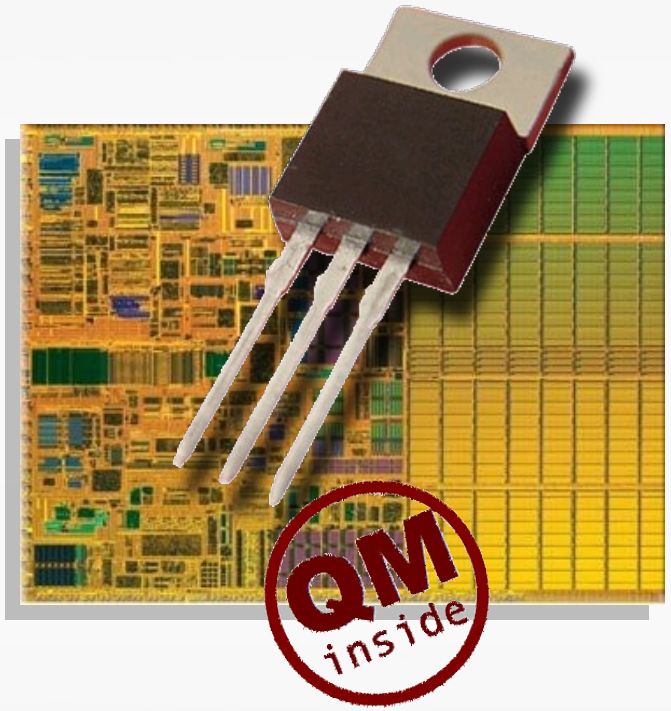




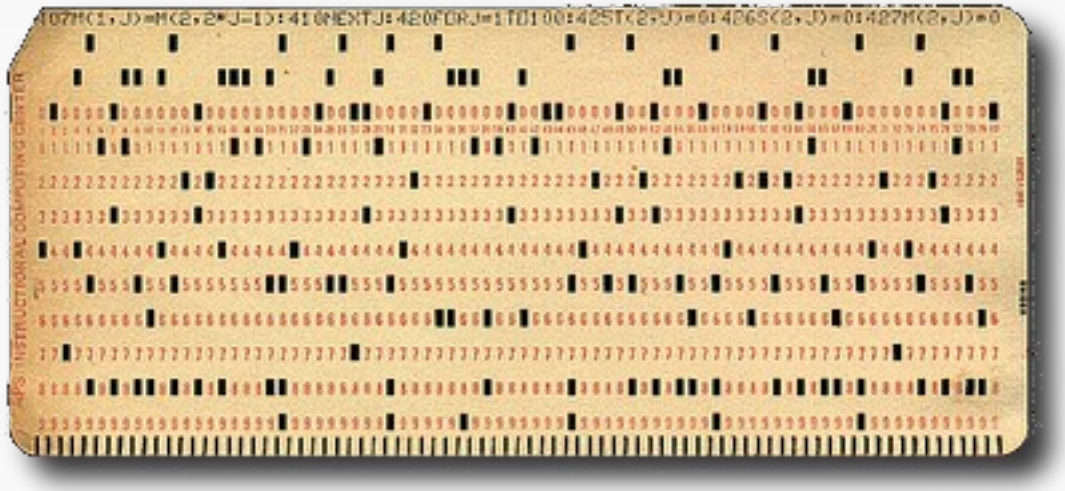
Los estados cuánticos se definen a partir de distribuciones de probabilidad.


PROBLEM
OPPORTUNITY

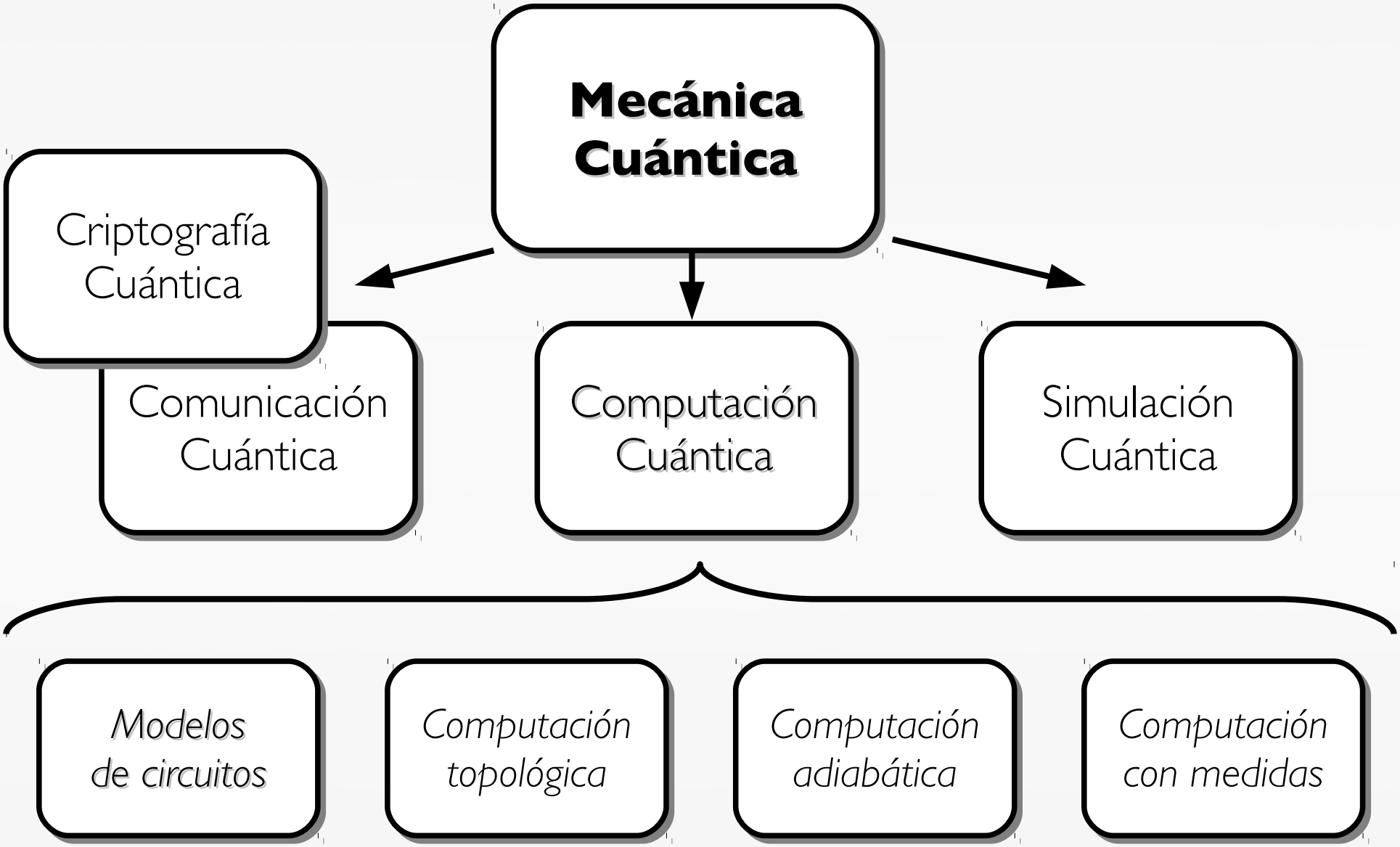
ORDENADORES



ORDENADORES

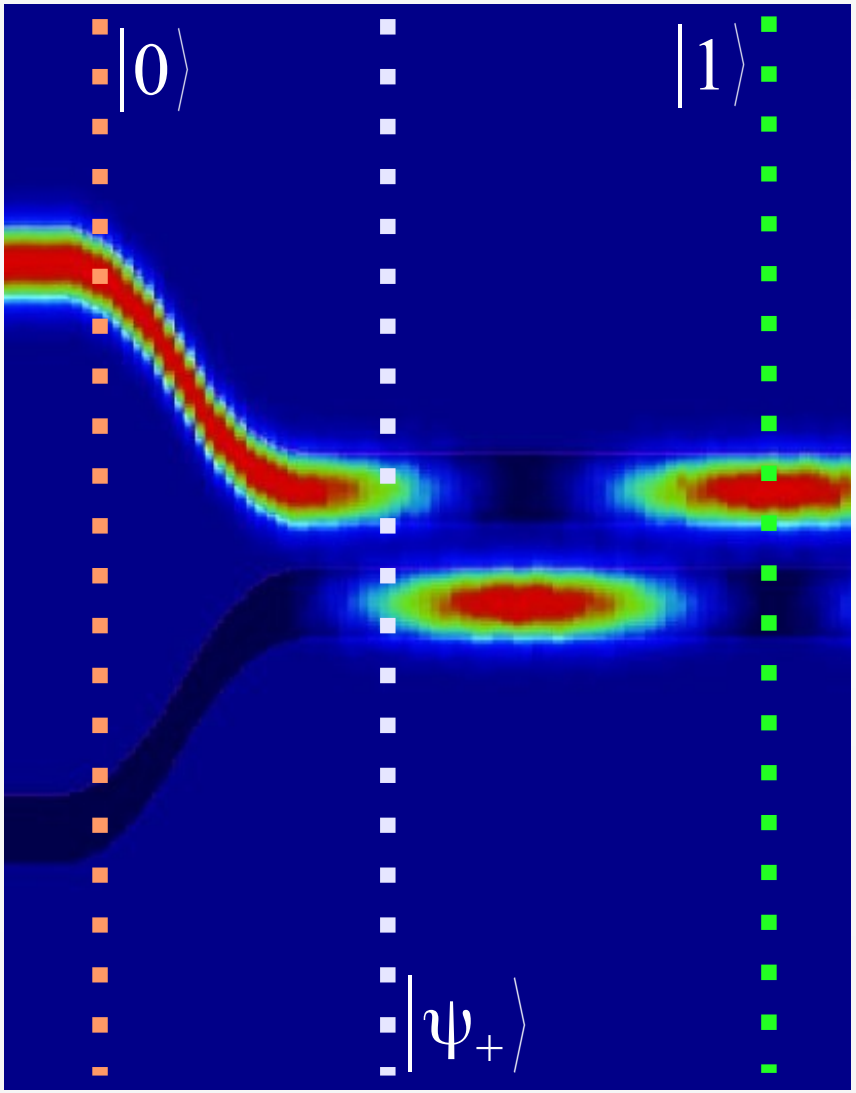


Tratamos a nuestros dispositivos cuánticos
como objetos clásicos.


Mecánica Cuántica
Criptografía Cuántica
Comunicación Cuántica
Computación Cuántica
Simulación Cuántica
Modelos de circuitos
Computación topológica
Computación adiabática
Computación con medidas

Información cuántica

*QU*BIT



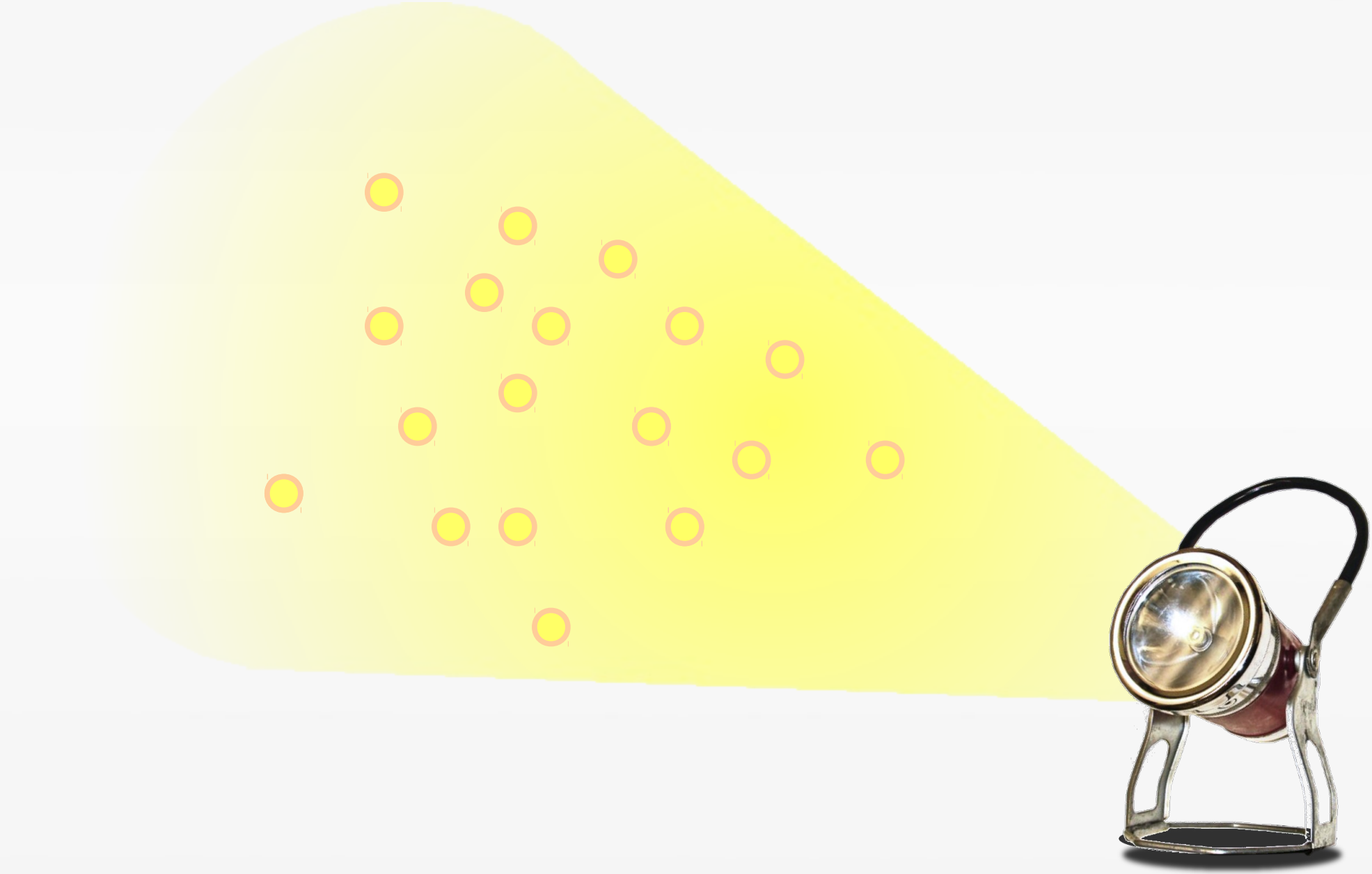
- Un sistema con dos estados disponibles, 0 y 1
- Se pueden crear los estados puros y superposición

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

$$|\psi_-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

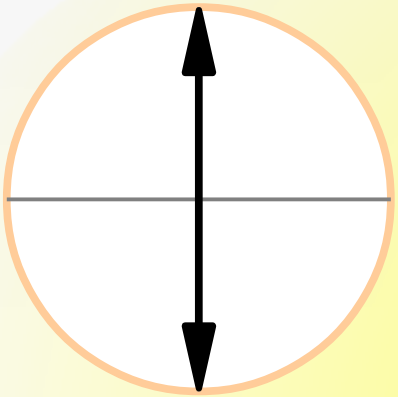
$$\frac{1}{\sqrt{2}} \times \frac{1}{\sqrt{2}} = \frac{1}{2} = 50\,\%$$

FOTONES

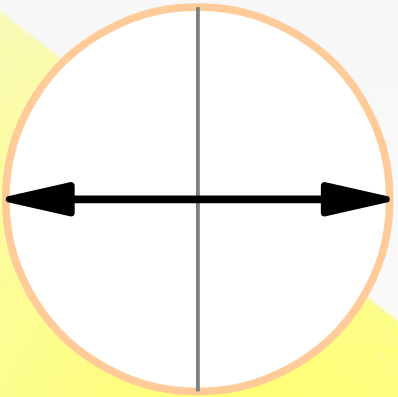


FOTONES

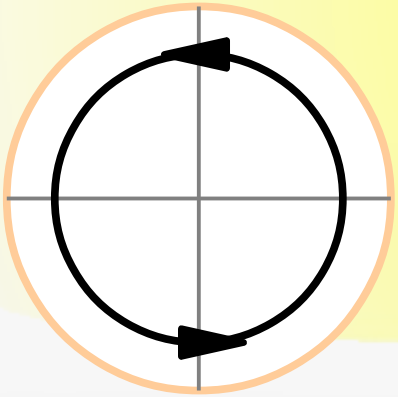
Vertical



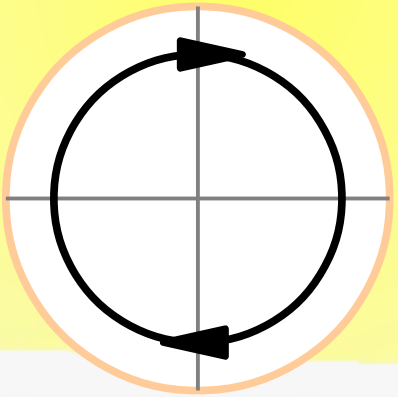
Horizontal



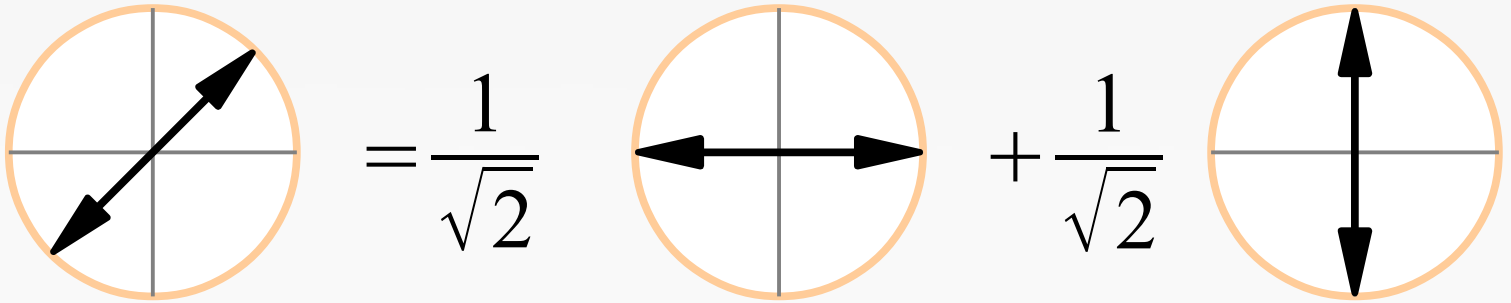
Izquierda

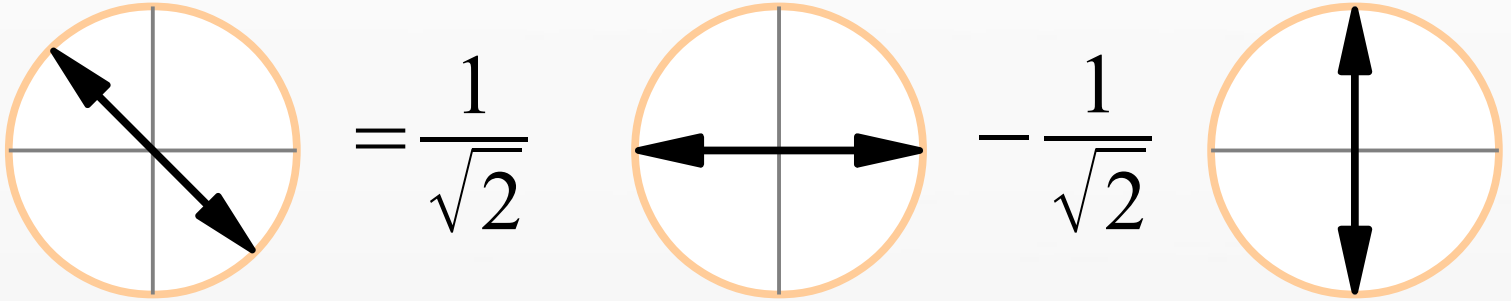


Derecha



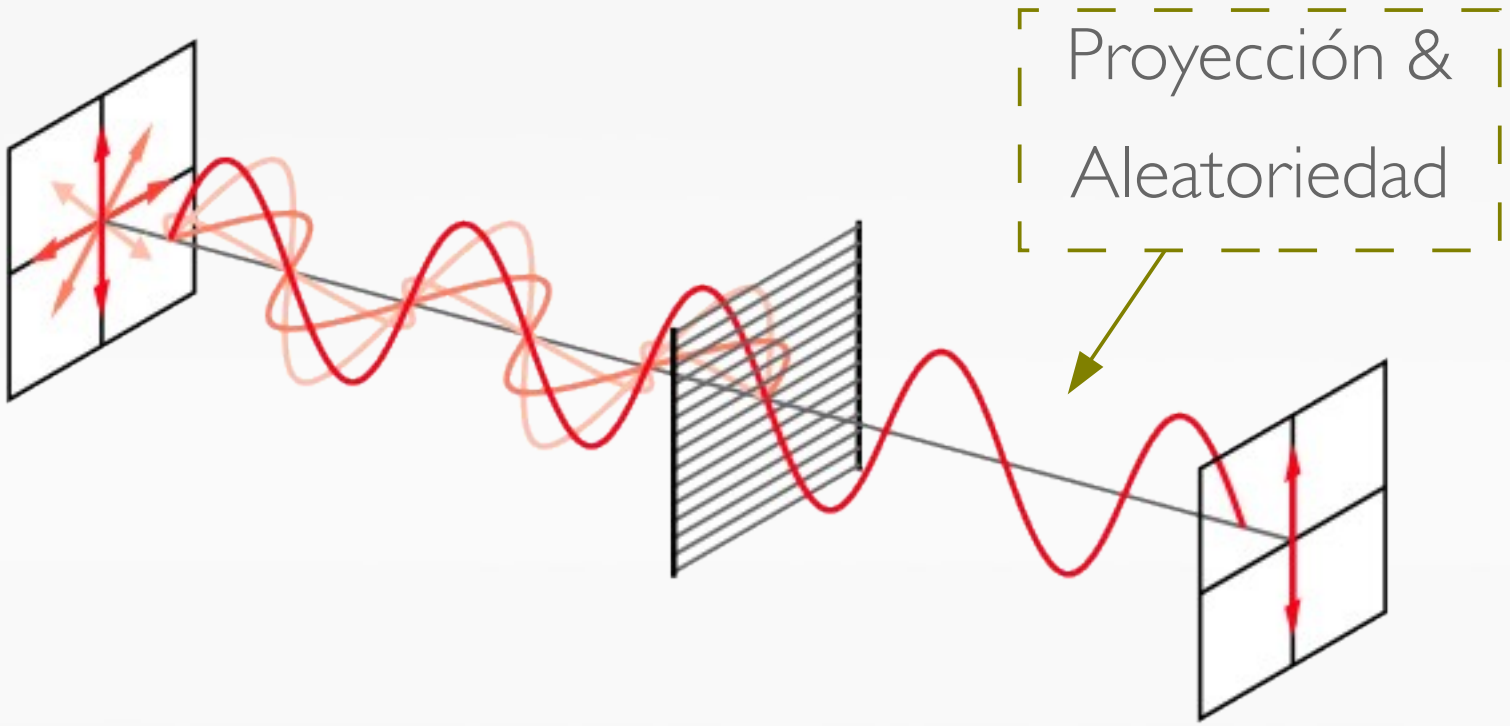
FOTONES

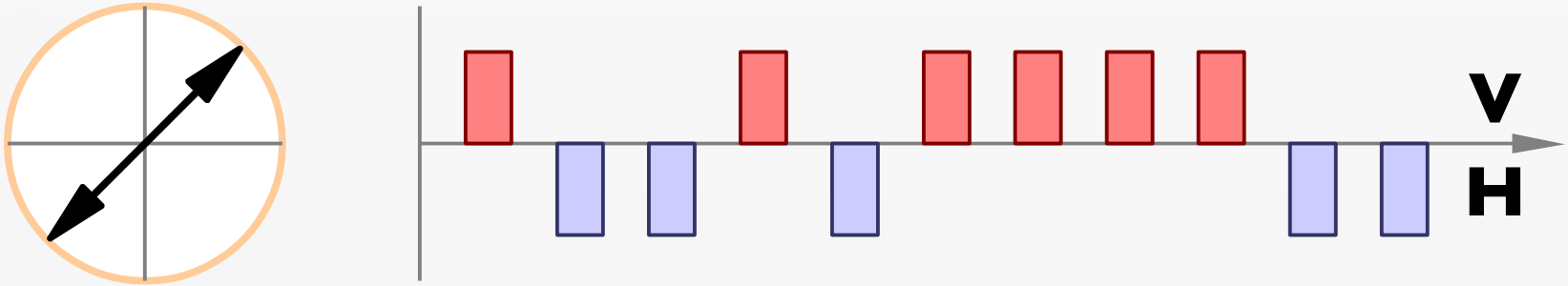




Superposición "cuántica"

MEDIDA

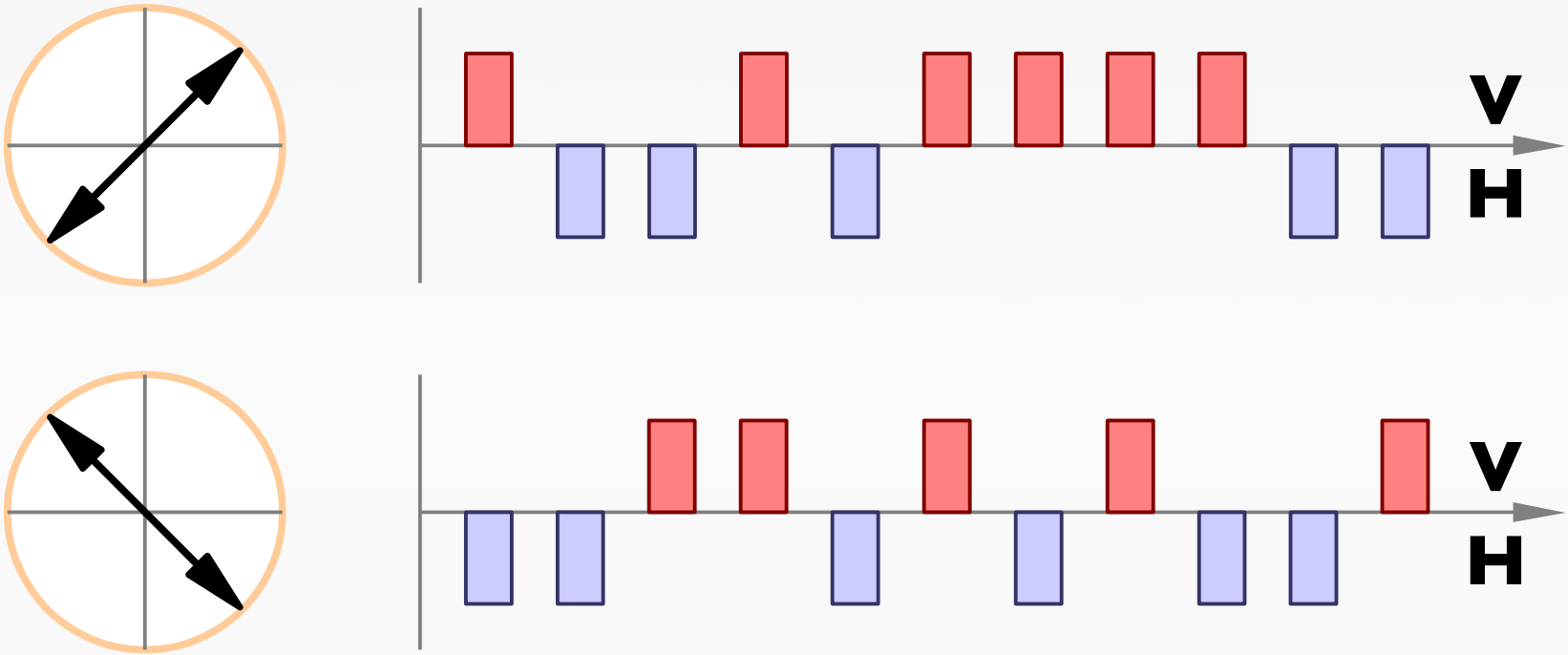




QM CHURCH

- Quantum phenomena do not occur in a Hilbert space, they occur in a laboratory.
- Quantum theory needs no 'interpretation'.
- Unperformed experiments have no results.
- Never underestimate the ingenuity of experimental physicists.

INDETERMINACIÓN



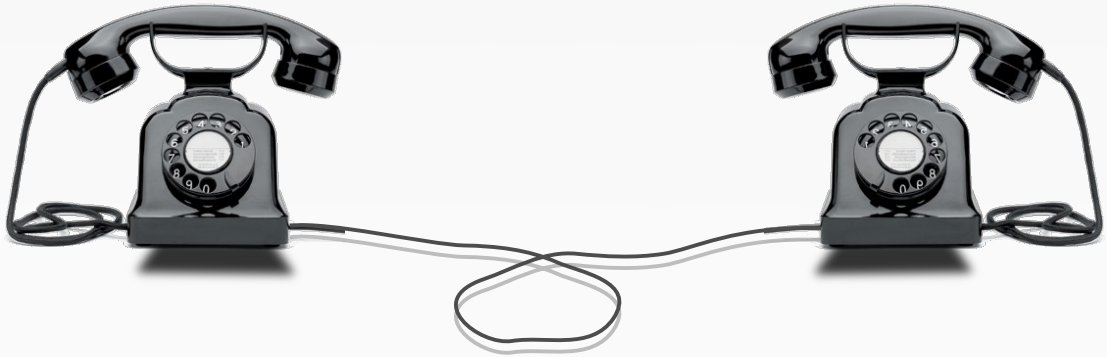
Medidas en una "base" no sirven para distinguir estados creados en otra base

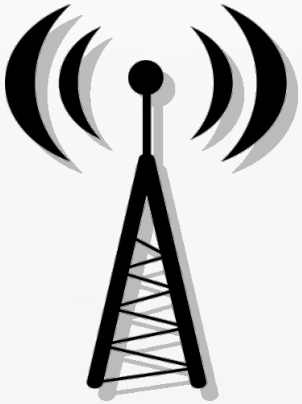
Criptografía cuántica

CRIPTOGRAFÍA

CRIPTOGRAFÍA

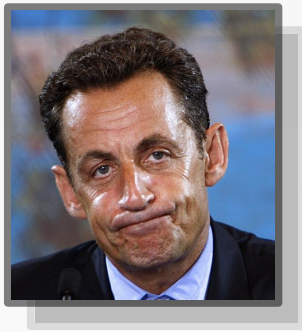
CRIPTOGRAFÍA





CLAVE PRIVADA

0 0 0 1 0 0 1 0 0 0 0 ...



Mensaje

1 0 1 1 1 0 0 1 1 0 1 ...

Q Key

1 0 1 0 1 0 1 1 1 0 1 ...

Transmisión

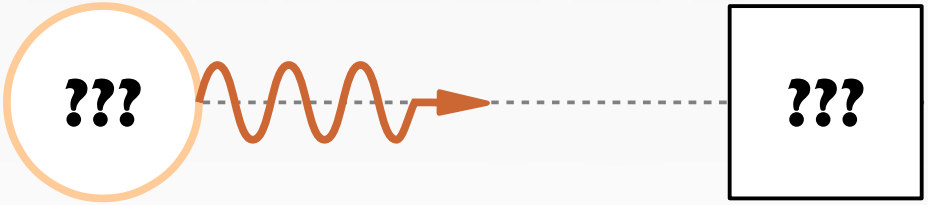
0 0 0 1 0 0 1 0 0 0 0 ...

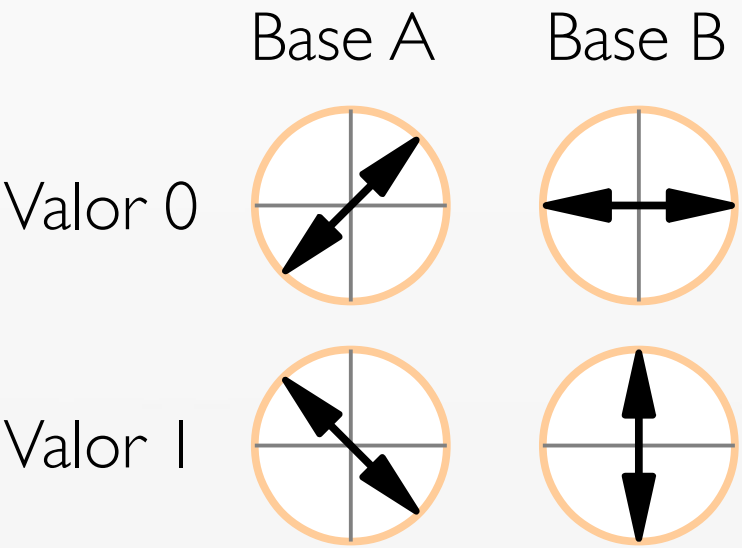
0 0 0 1 0 0 1 0 0 0 0 ...

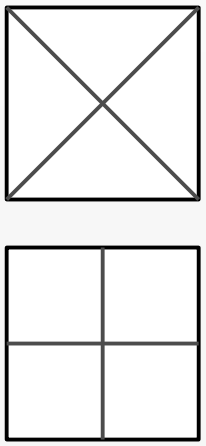
1 0 1 0 1 0 1 1 1 0 1 ...

1 0 1 1 1 0 0 1 1 0 1 ...

CRIPTOGRAFÍA







Medida A

Medida B

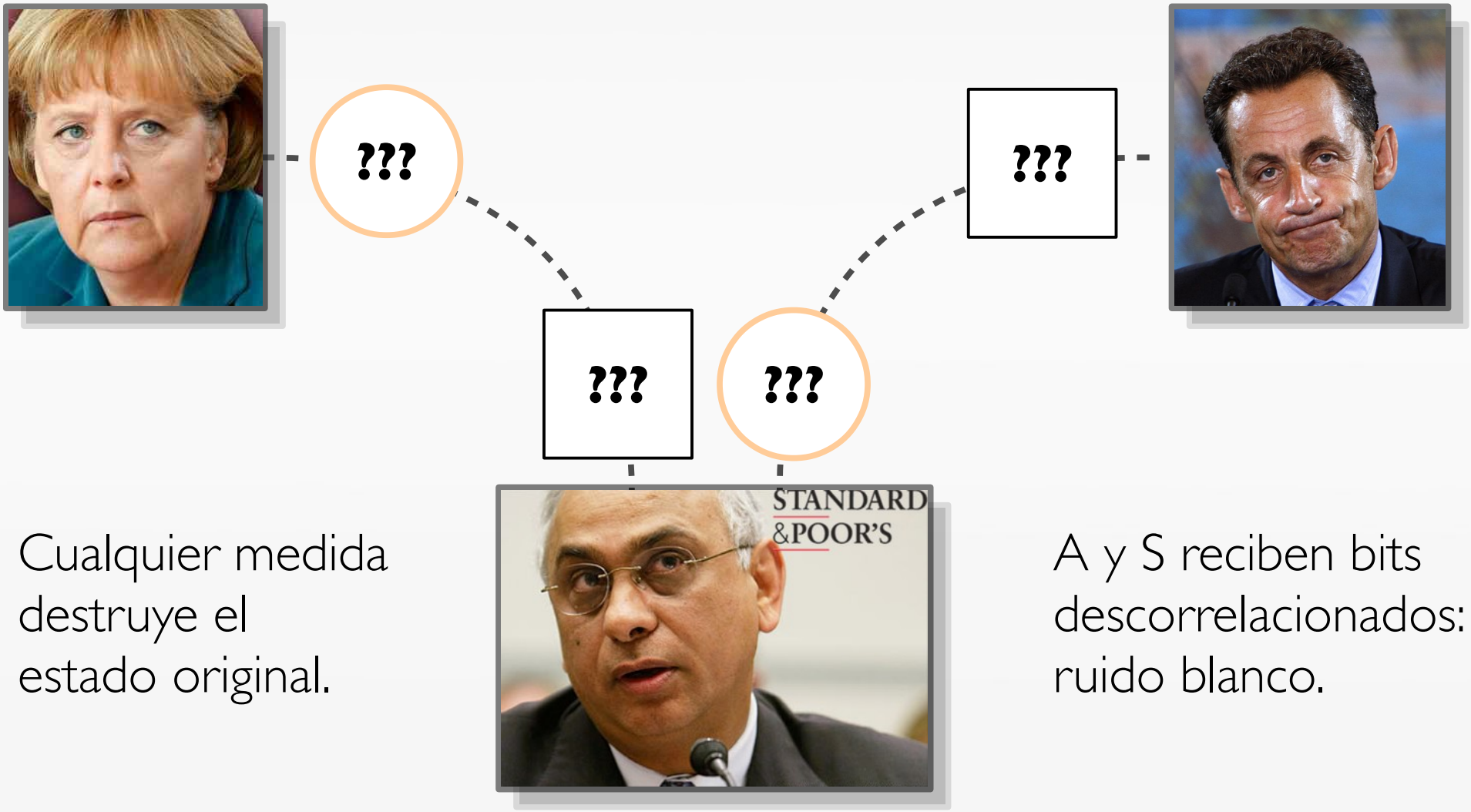
CRIPTOGRAFÍA

- Angela escoge una base (A/B) y un valor (0/1) aleatoriamente.
- Sarko escoge una base (A/B) aleatoriamente
- El fotón se envía y mide.
- Se repite muchas veces.
- A y S comunican las bases.
- Se guardan los bits sólo cuyas bases coinciden.

CRIPTOGRAFÍA

Base A	Base S.	Emitido	Recibido	OK?
A	A	I	I	✓
A	B	0	I	✗
B	A	I	0	✗
A	A	I	I	✓
B	A	0	0	✗
B	B	0	0	✓
B	A	I	0	✗
A	A	I	I	✓
B	A	0	0	✗

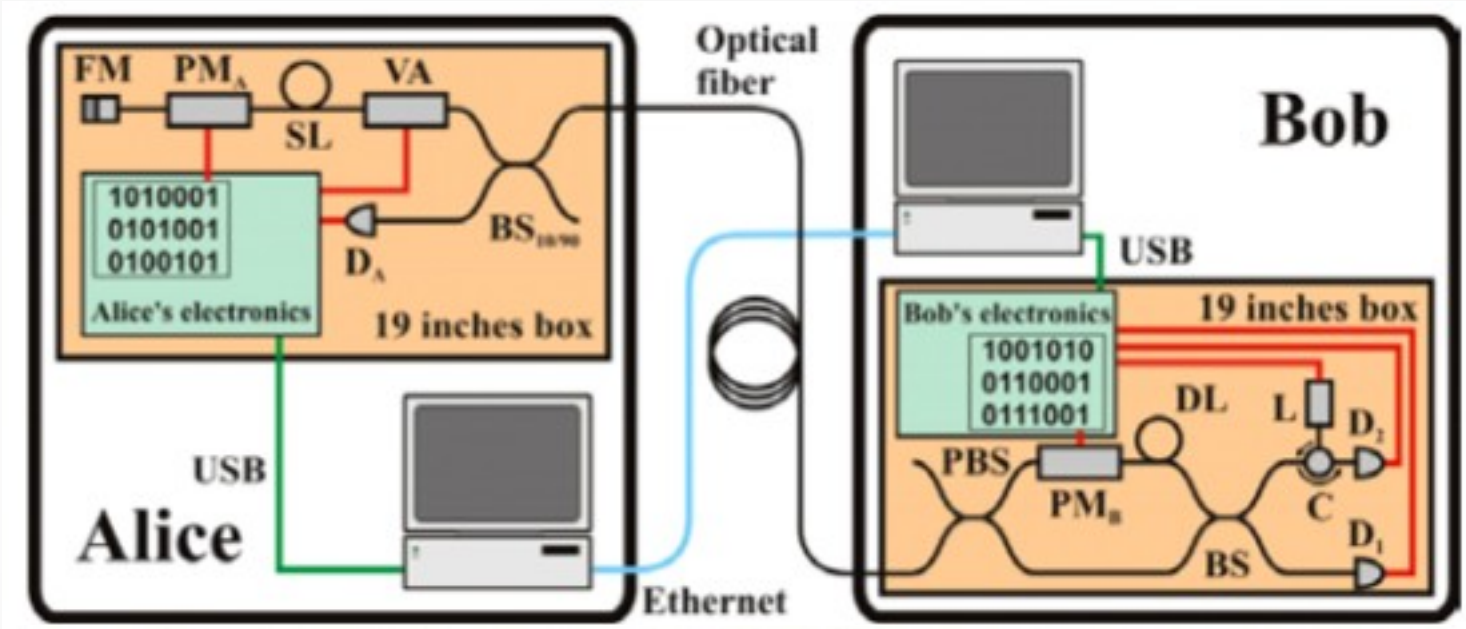
SEGURIDAD

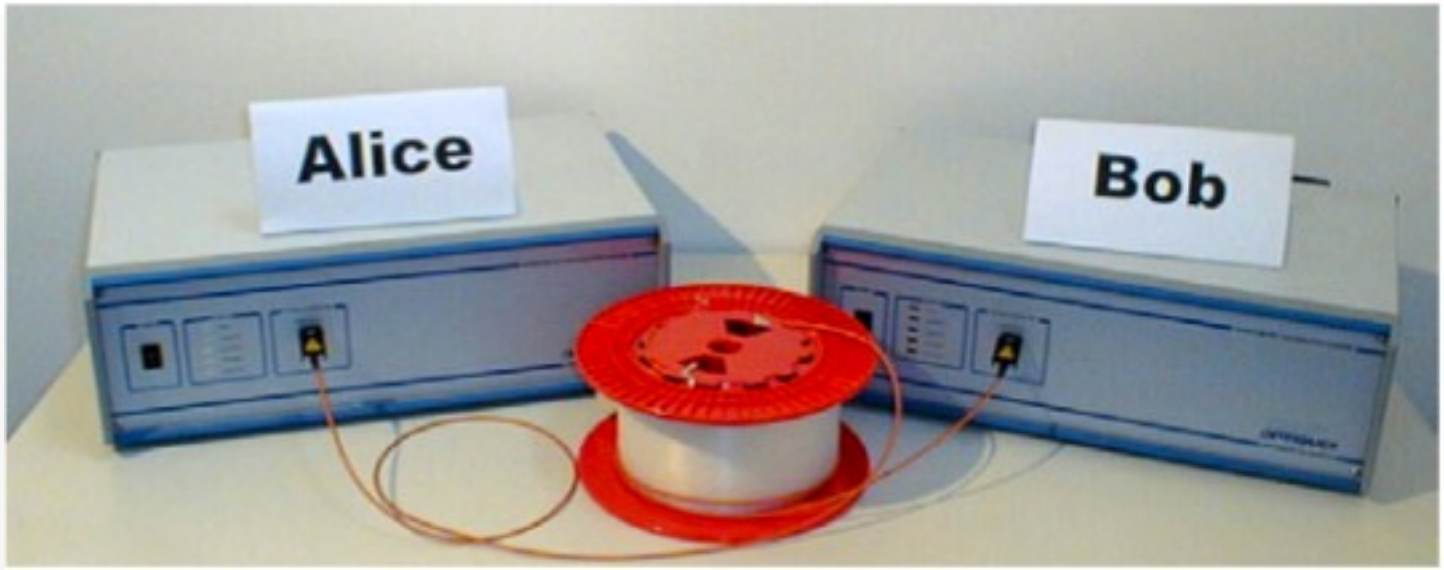


Cualquier medida destruye el estado original.

A y S reciben bits descorrelacionados: ruido blanco.

DISPOSITIVOS





DISPOSITIVOS

IDQ
FROM VISION TO TECHNOLOGY

USER CASE

REPUBLIC AND STATE OF GENEVA
POST TENEBRAS LUX

REDEFINING SECURITY

Geneva Government

Secure Data Transfer for Elections

Gigabit Ethernet Encryption with Quantum Key Distribution

IDQ
FROM VISION TO TECHNOLOGY

USER CA

REDEFINING SECURITY

Global Bank

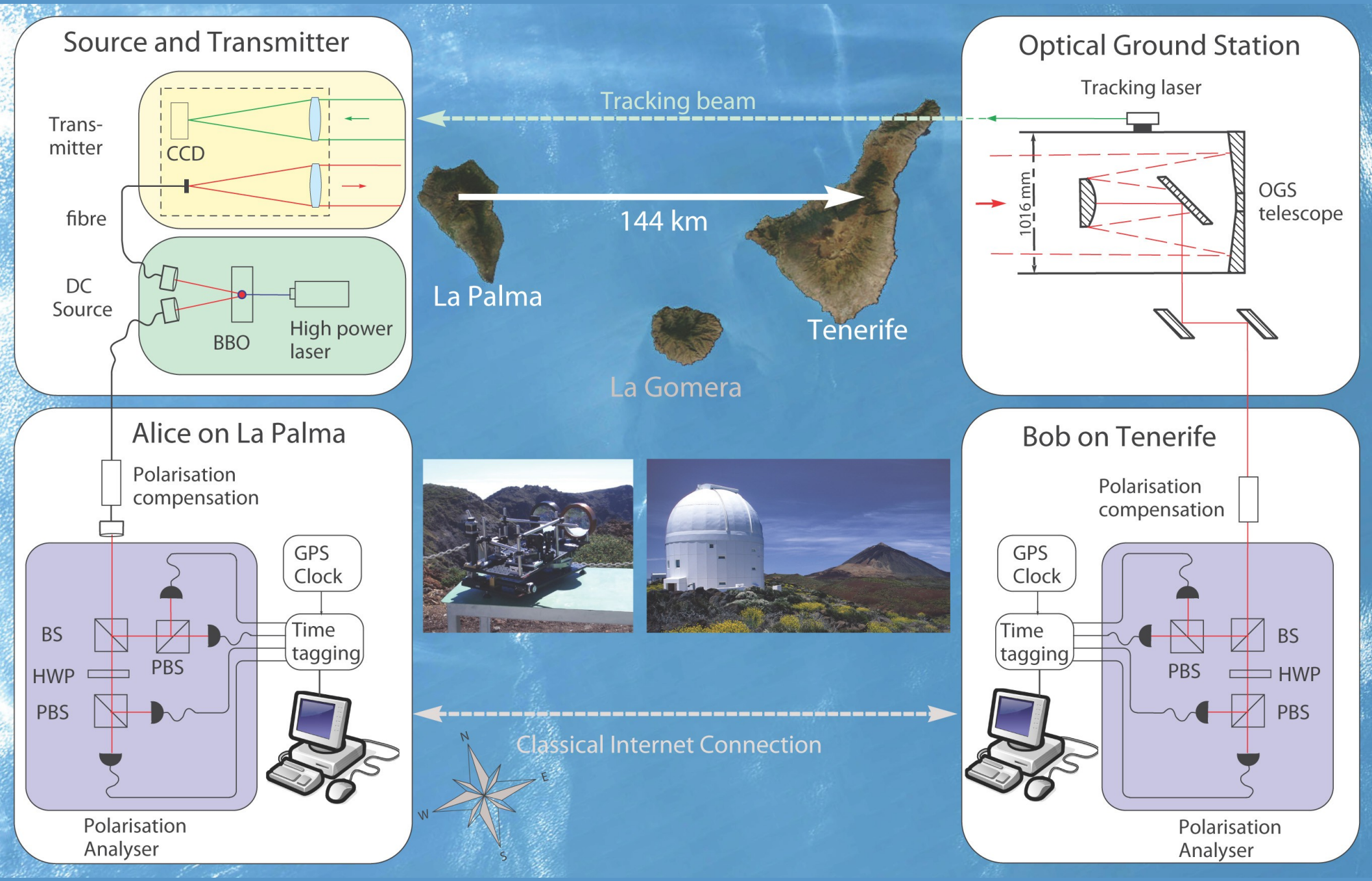
IDQ Secures Global Wide Area Network

Multipoint 100 Megabit Ethernet Encryption

UNIVERSIDAD POLITÉCNICA MADRID

POLITÉCNICA

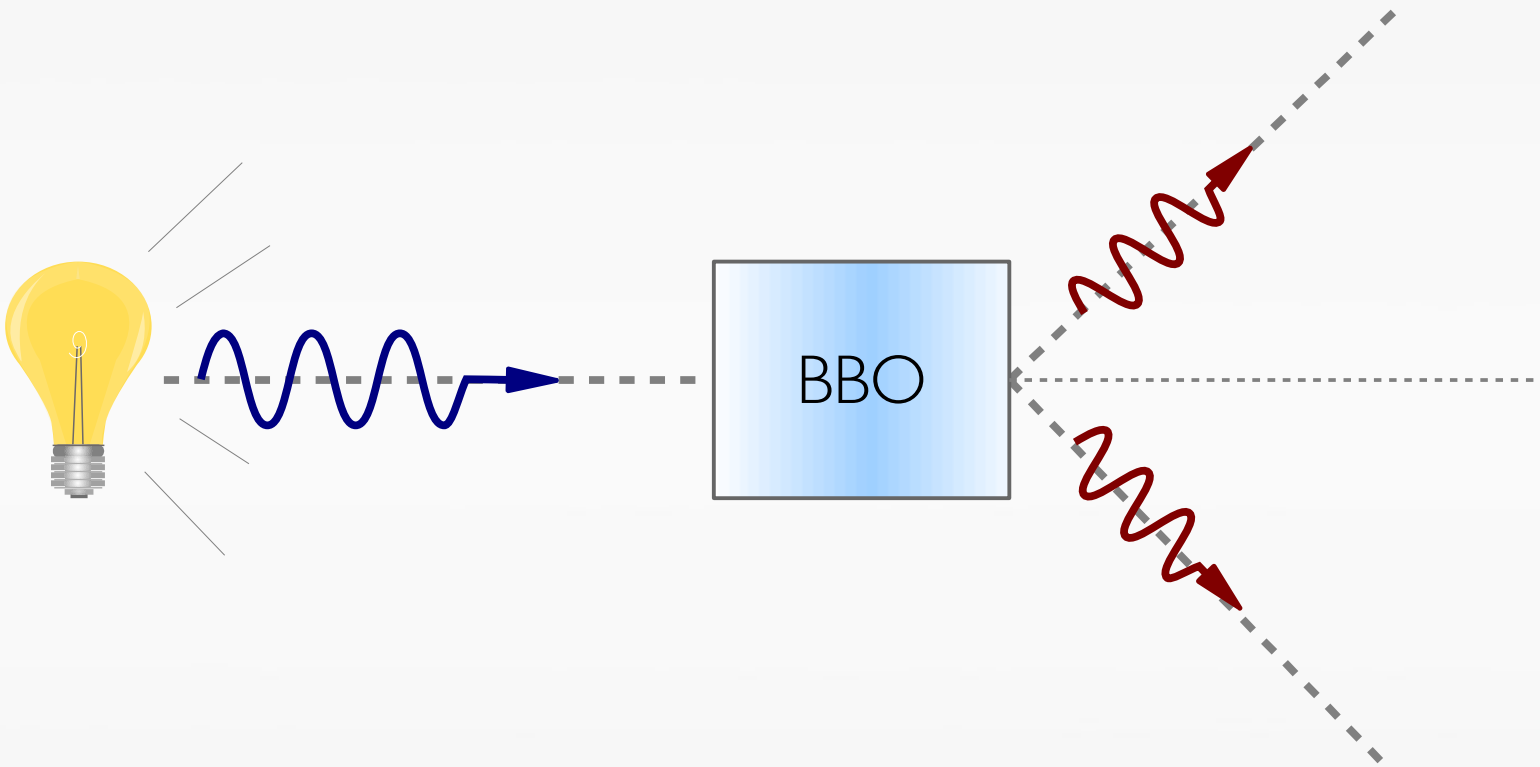
Telefonica


Source and Transmitter
Trans-
mitter
CCD
fibre
DC
Source
BBO
High power
laser
Tracking beam
144 km
La Palma
Tenerife
La Gomera
Optical Ground Station
Tracking laser
1016 mm
OGS
telescope
Alice on La Palma
Polarisation
compensation
GPS
Clock
BS
HWP
PBS
PBS
Time
tagging
Polarisation
Analyser
Classical Internet Connection
Bob on Tenerife
Polarisation
compensation
GPS
Clock
Time
tagging
BS
PBS
HWP
PBS
Polarisation
Analyser

Entrelazamiento

CORRELACIONES

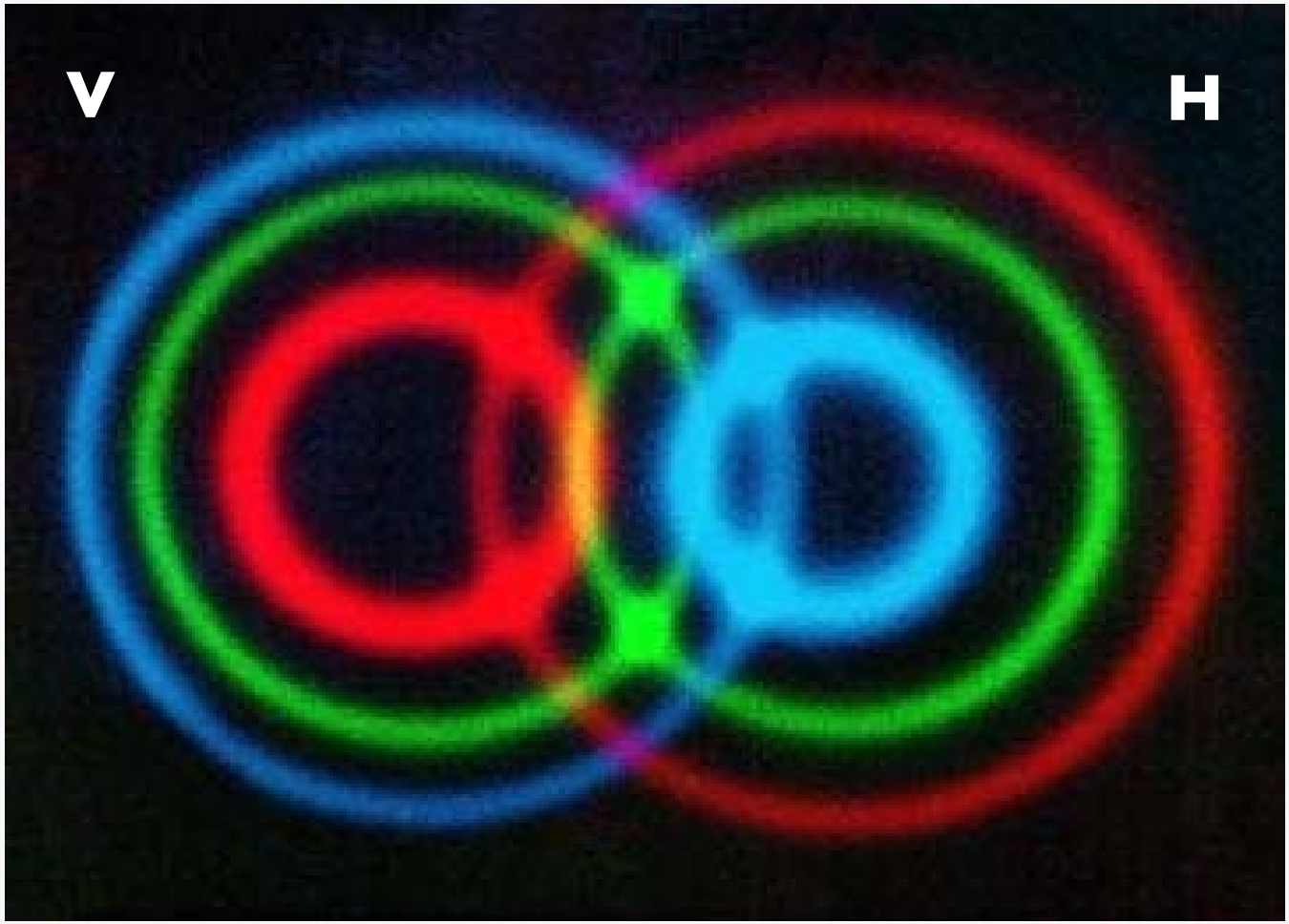
PARES DE FOTONES



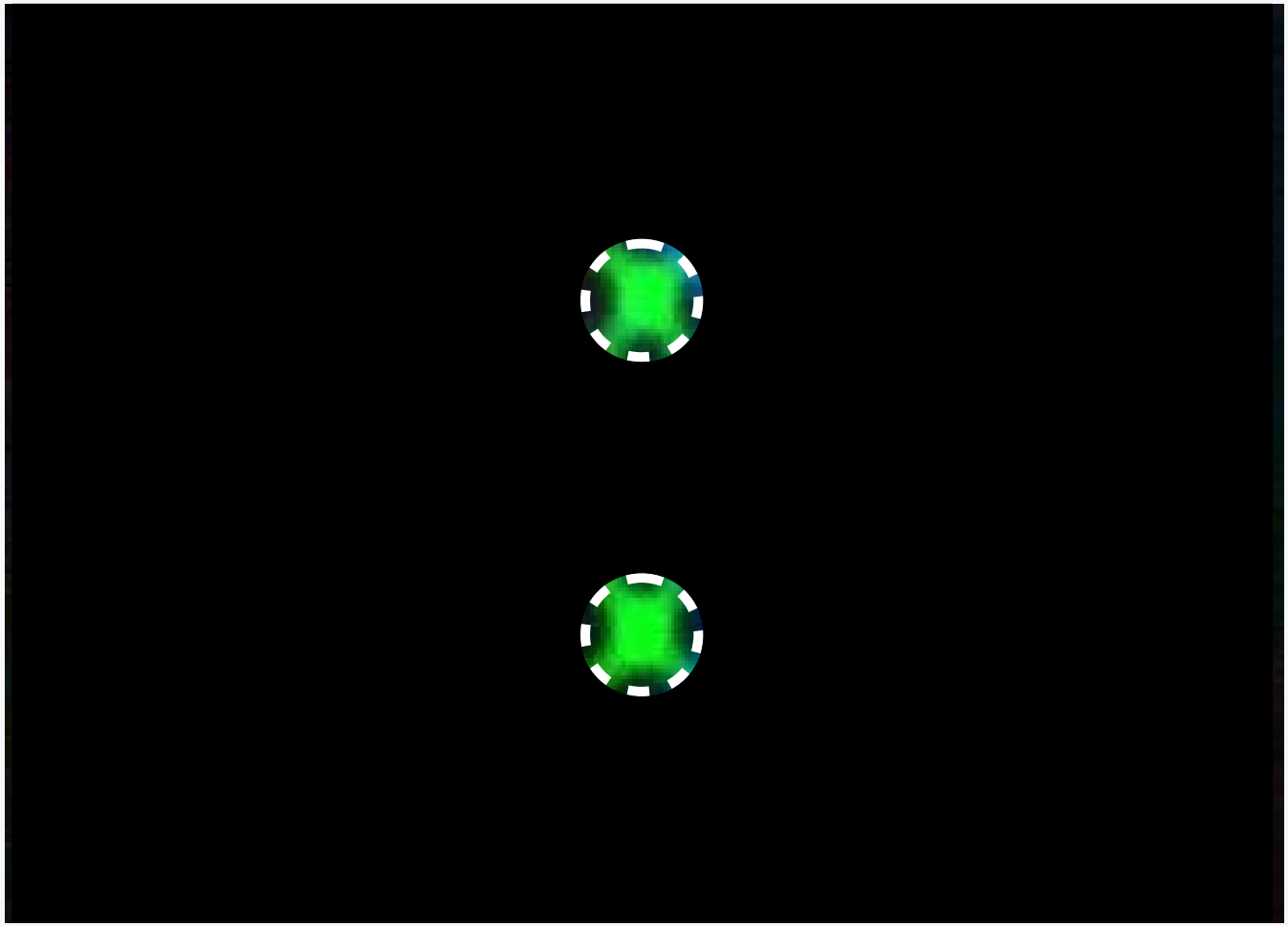
"Parametric down conversion" =

"doblado de fotones"

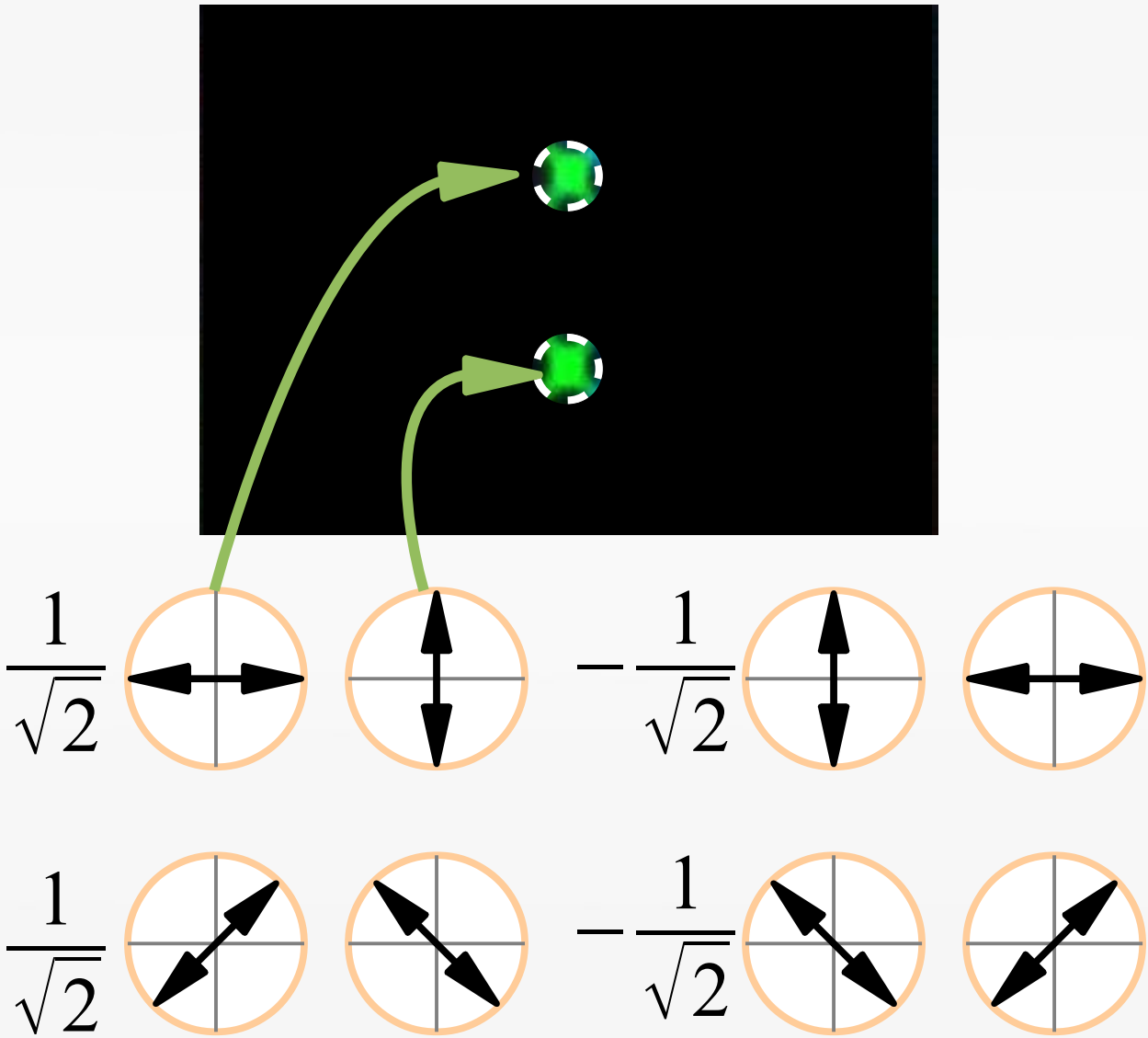
POLARIZACIÓN



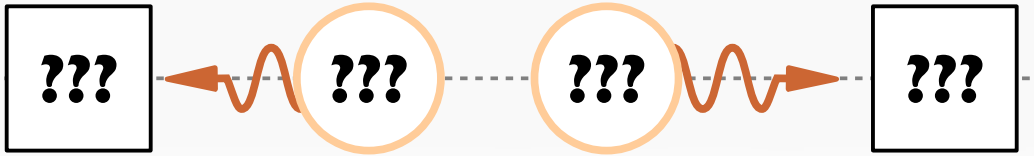
ENTRELAZAMIENTO

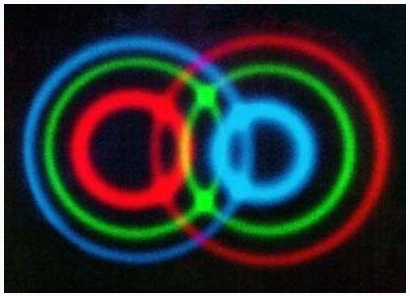


ENTRELAZAMIENTO

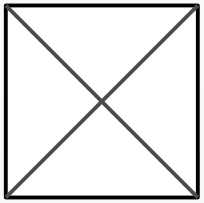


CRIPTOGRAFÍA

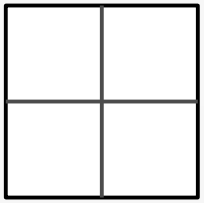


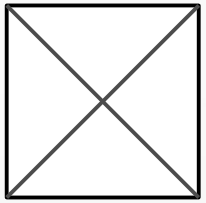


Medida A

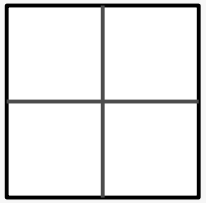


Medida B





Medida A

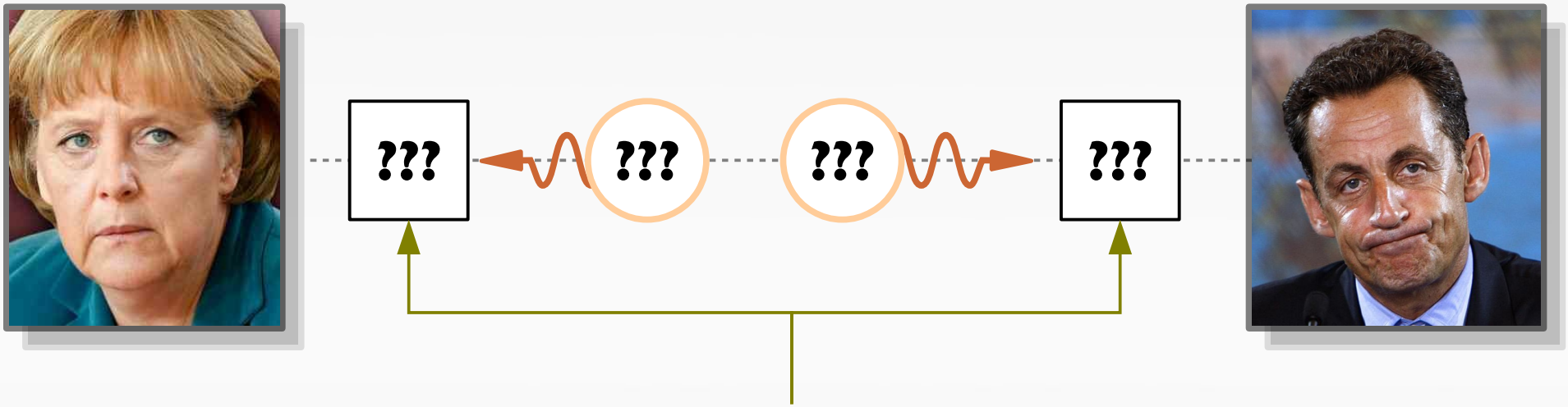


Medida B

CRIPTOGRAFÍA

Base A	Base S	Bit A	Bit B	OK?
A	A	I	0	✓
A	B	0	I	✗
B	A	I	0	✗
A	A	0	I	✓
B	A	0	0	✗
B	B	0	I	✓
B	A	I	0	✗
A	A	I	0	✓
B	A	0	0	✗

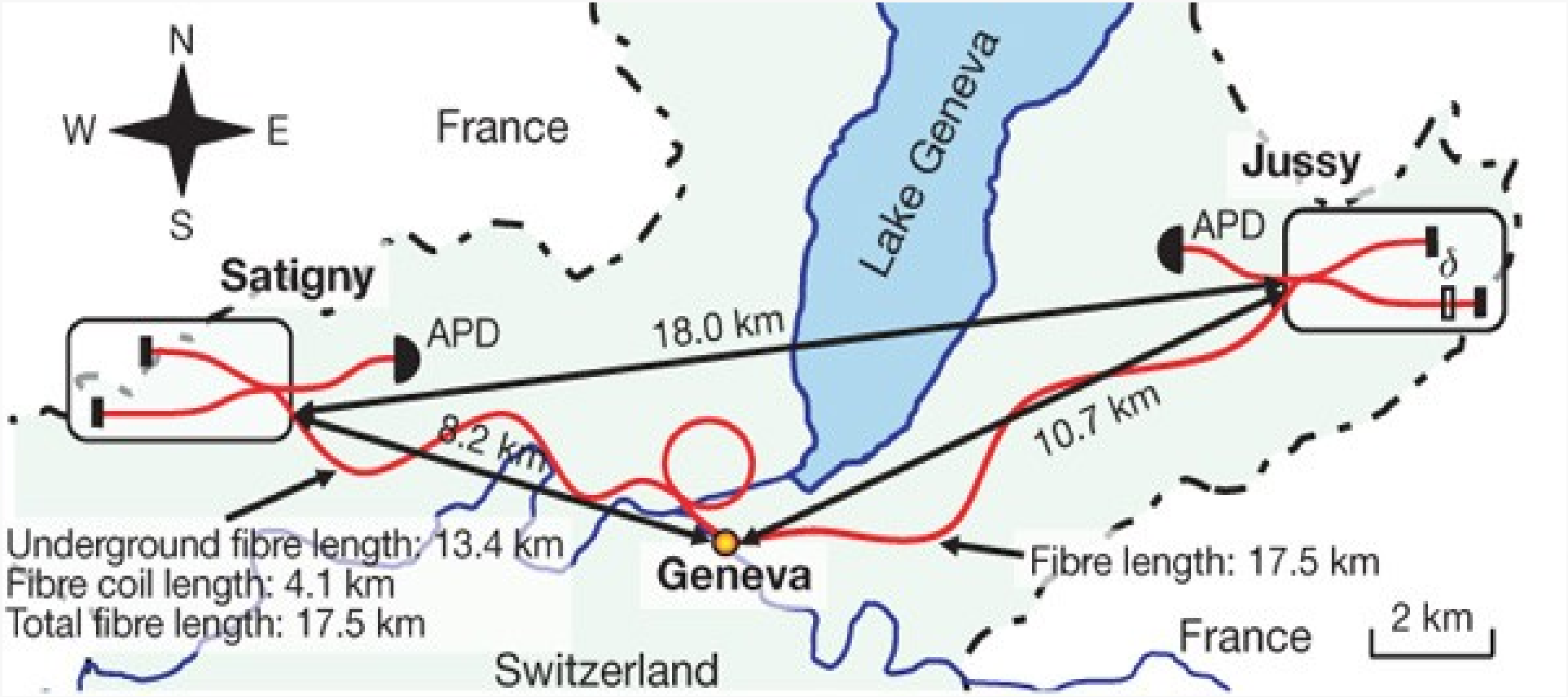
ACCIÓN A DISTANCIA?



Correlaciones mayores que clásicamente:
independientes de la base.

"Influencia mutua"?
Se hablan los fotones?

NO!

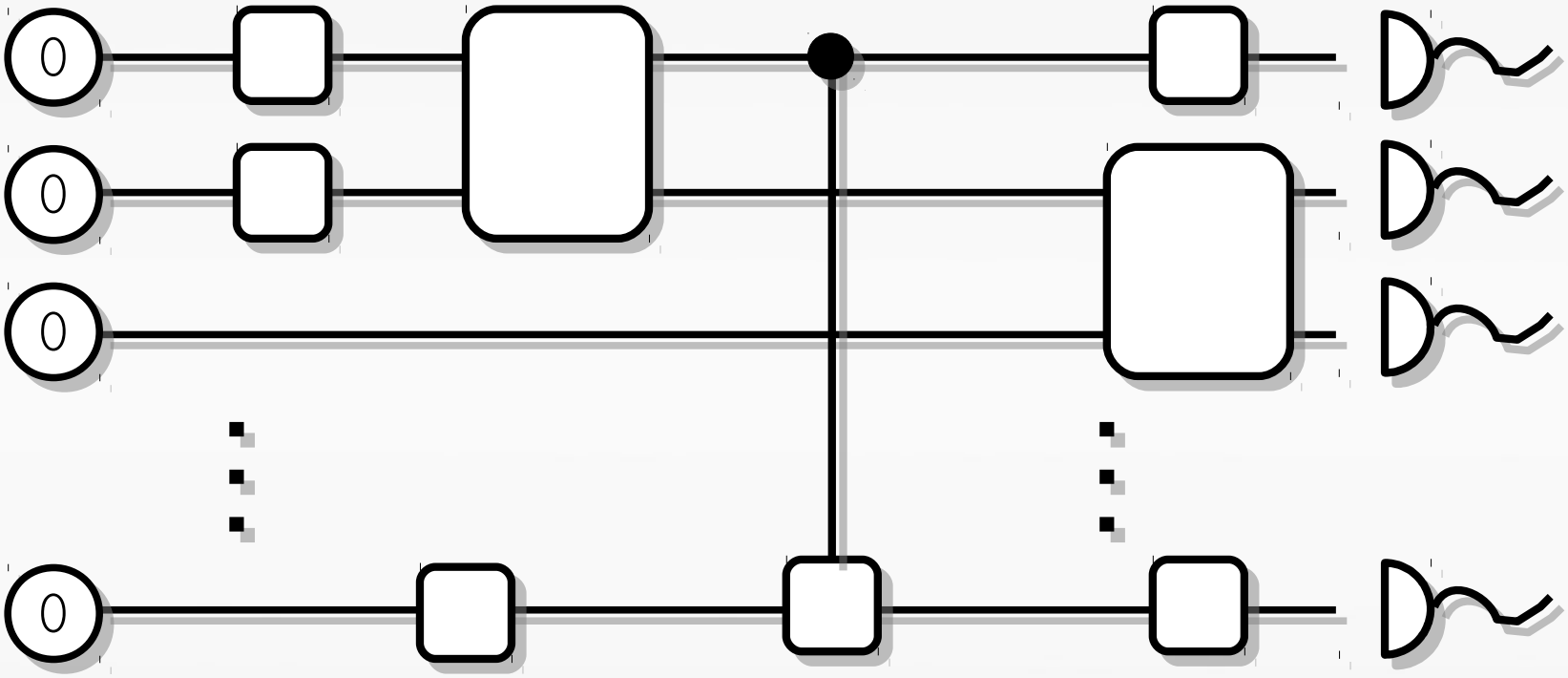

N
W
E
S
France
Lake Geneva
Jussy
APD
δ
Satigny
APD
18.0 km
8.2 km
10.7 km
Underground fibre length: 13.4 km
Fibre coil length: 4.1 km
Total fibre length: 17.5 km
Geneva
Fibre length: 17.5 km
France
2 km
Switzerland

100.000 × c ???

Computación

¿PROBABILISTA
=
IMPRECISO?

ALGORITMOS



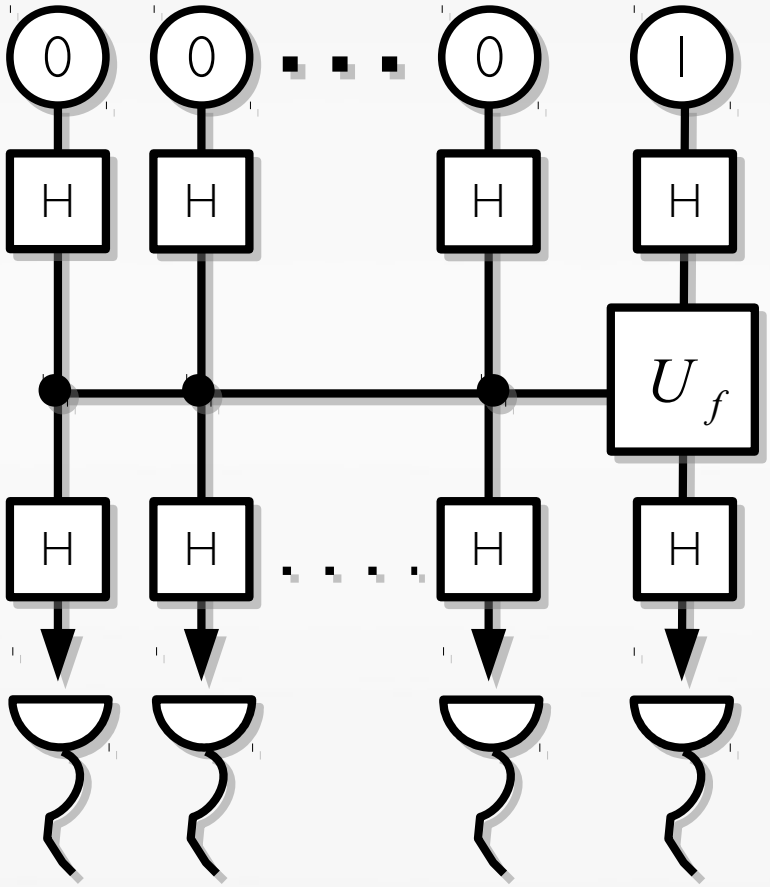
POTENCIAL

$$|\psi\rangle = c_{000\ldots0}|000\ldots0\rangle + c_{000\ldots1}|000\ldots1\rangle + \ldots + c_{111\ldots1}|111\ldots1\rangle$$

- Paralelismo implícito
- Complejidad exponencial

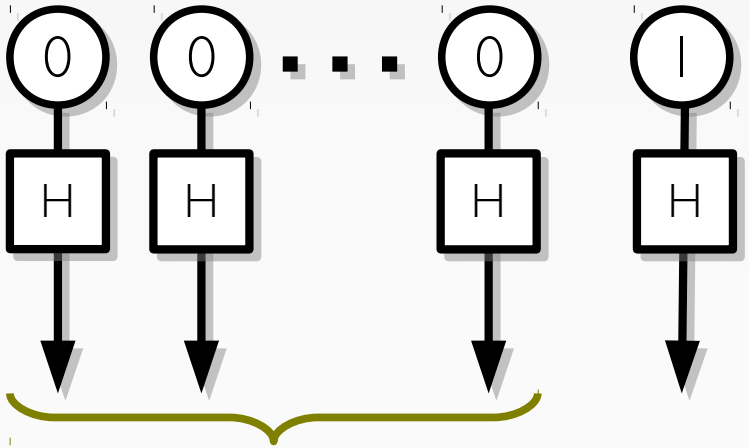
ALGORITMOS

- Determinar si una función de varias variables está "balanceada"
  - O bien es constante
  - O emite el mismo número de 0 y 1
- Clásicamente necesitamos hasta $2^{N/2}$ operaciones
- Cuánticamente, sólo 3 pasos.



PARALELISMO

Con una sola operación, preparamos todos los números posibles



$$\frac{1}{\sqrt{N}}|000\ldots0\rangle +$$

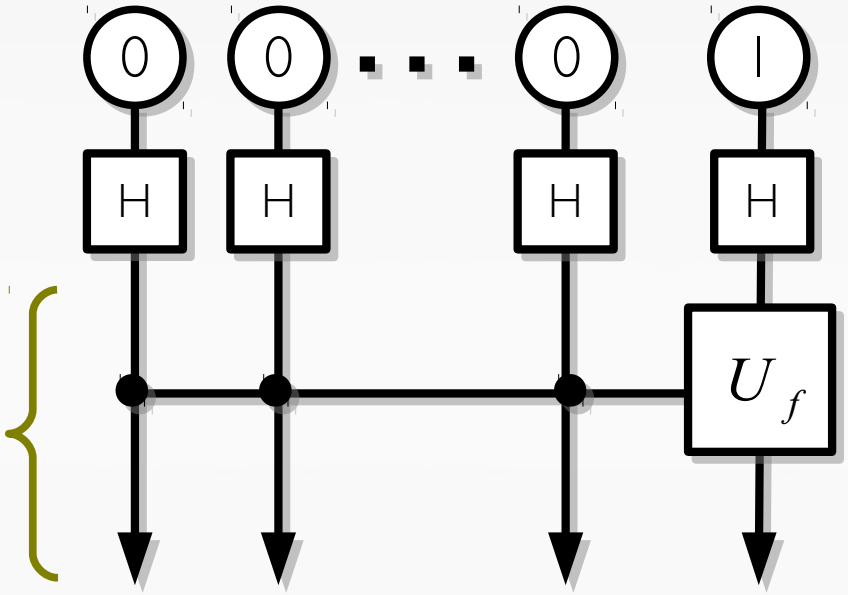
$$\frac{1}{\sqrt{N}}|000\ldots1\rangle + \ldots$$

$$\frac{1}{\sqrt{N}}|111\ldots1\rangle$$

PARALELISMO

El testigo extrae información sobre todos los cálculos posibles.

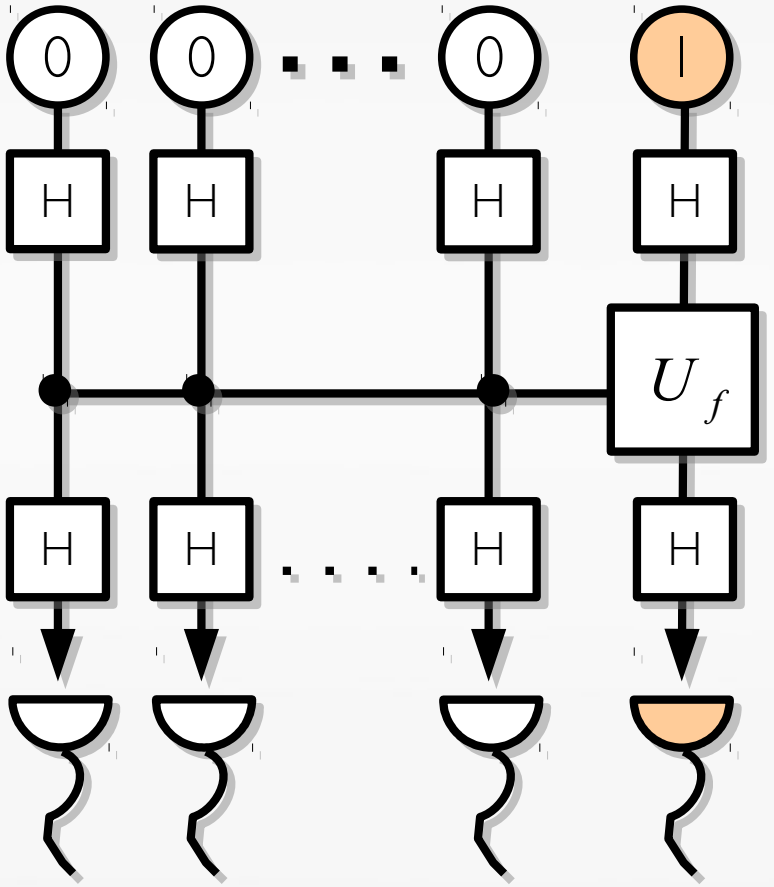
$$|a\,b\,c\ldots z\rangle|1\rangle$$
$$\downarrow$$
$$|a\,b\,c\ldots z\rangle|f(a,b,c\ldots z)\rangle$$



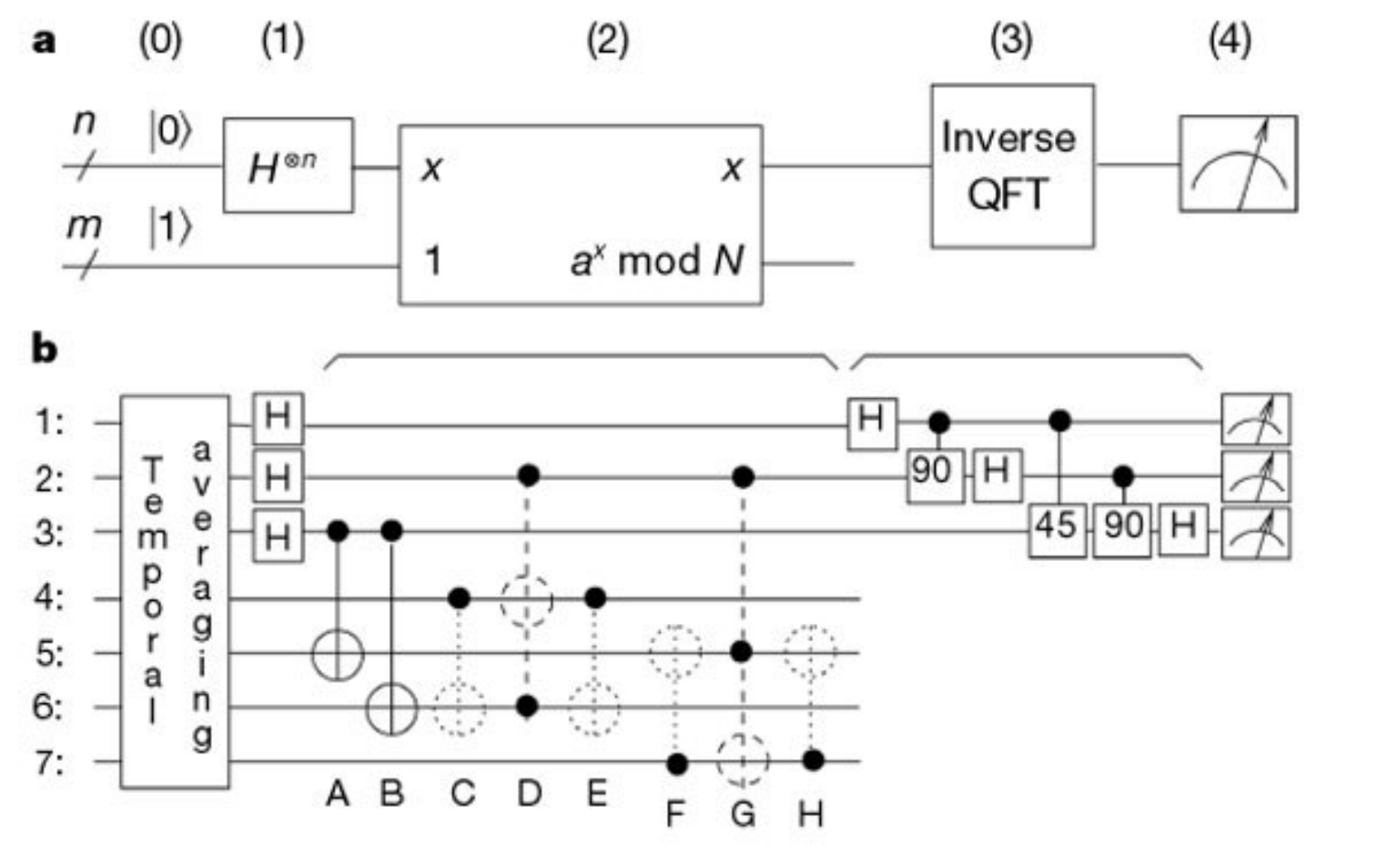
PARALELISMO

Al final el resultado en el testigo es

1 = la función es par
0 = la función es constante

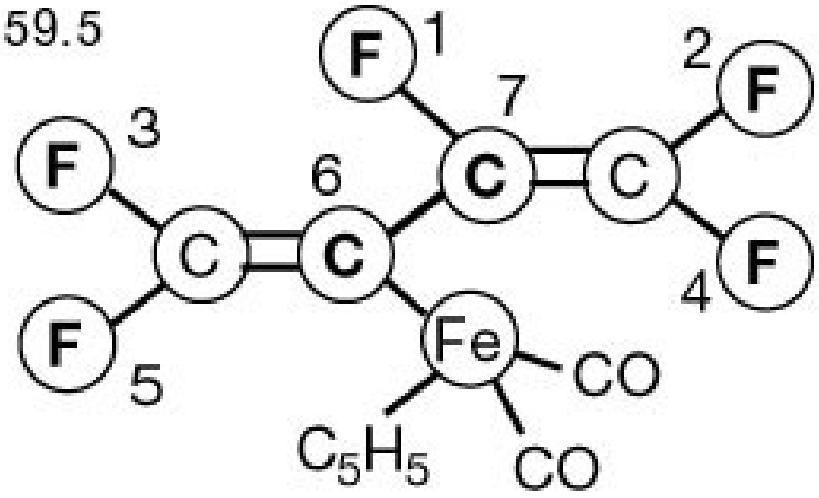


ALGORITMO DE SHOR

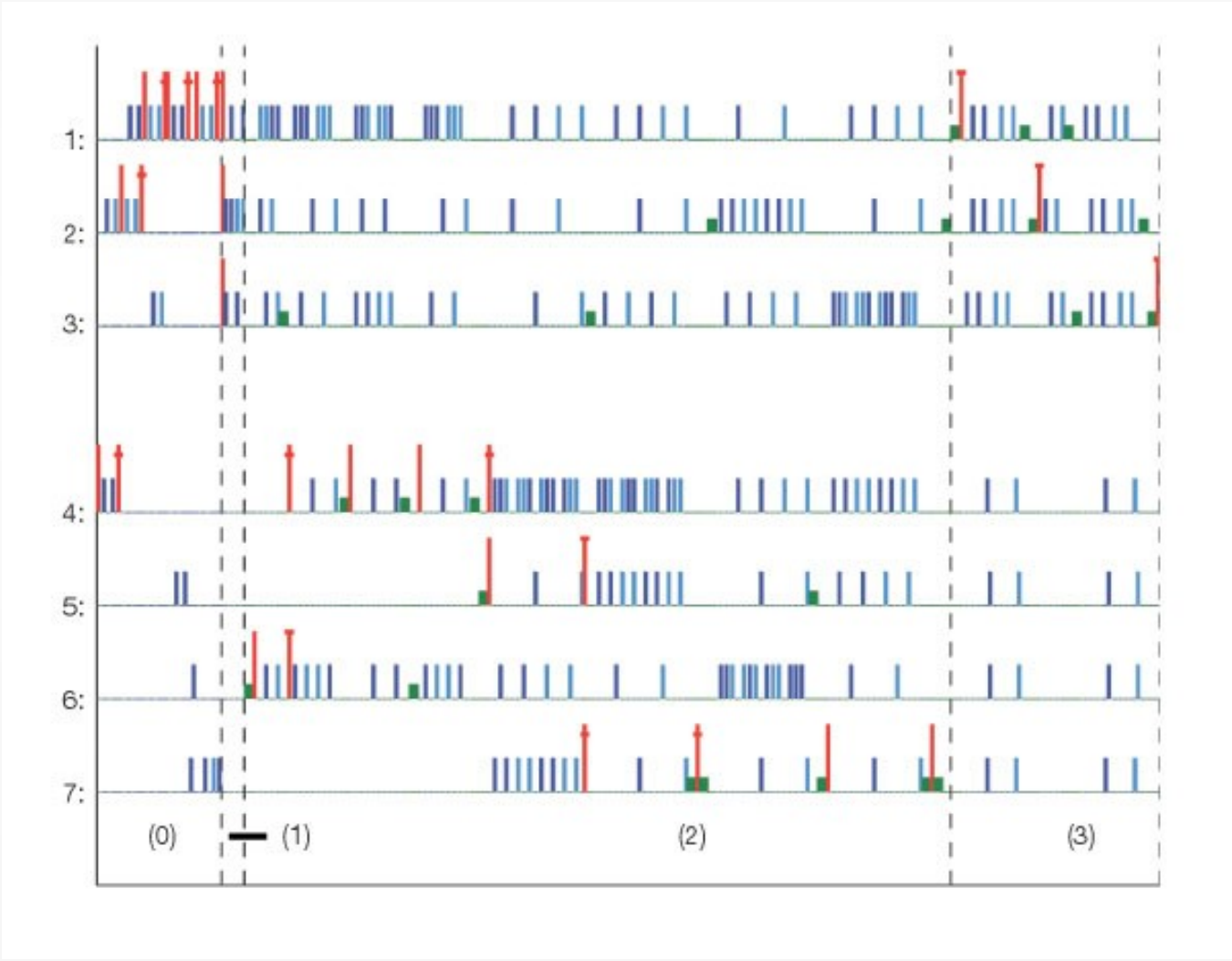


ALGORITMO DE SHOR

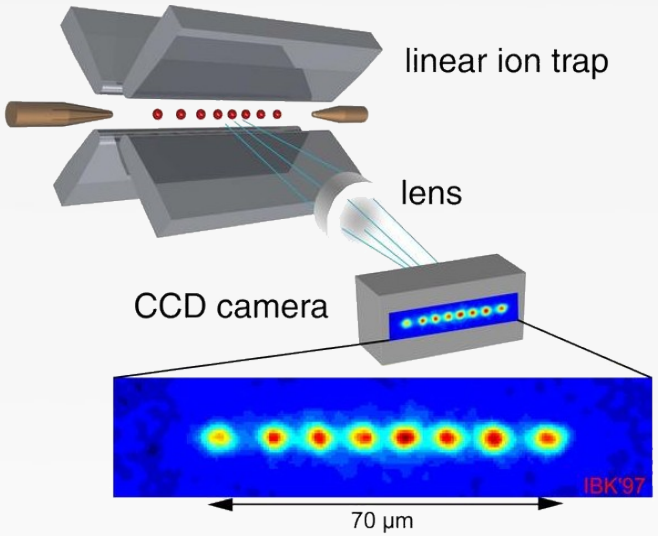
i	$\omega_i/2\pi$	$T_{1,i}$	$T_{2,i}$	J_{7i}	J_{6i}	J_{5i}	J_{4i}	J_{3i}	J_{2i}
1	–22052.0	5.0	1.3	–221.0	37.7	6.6	–114.3	14.5	25.16
2	489.5	13.7	1.8	18.6	–3.9	2.5	79.9	3.9	
3	25088.3	3.0	2.5	1.0	–13.5	41.6	12.9		
4	–4918.7	10.0	1.7	54.1	–5.7	2.1			
5	15186.6	2.8	1.8	19.4	59.5				
6	–4519.1	45.4	2.0	68.9					
7	4244.3	31.6	2.0						

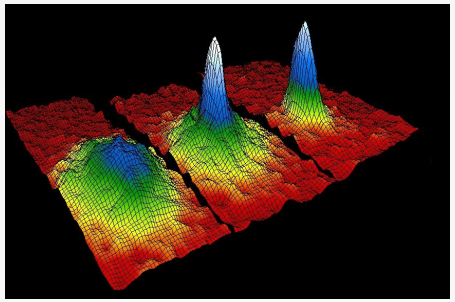


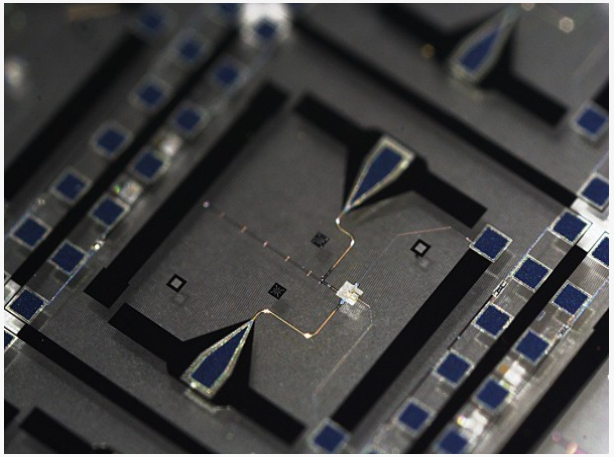
ALGORITMO DE SHOR



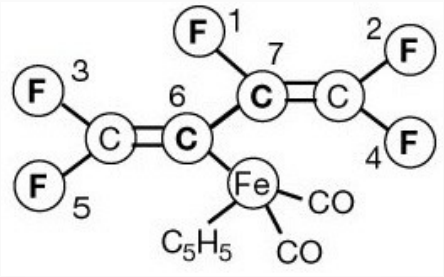
Implementaciones

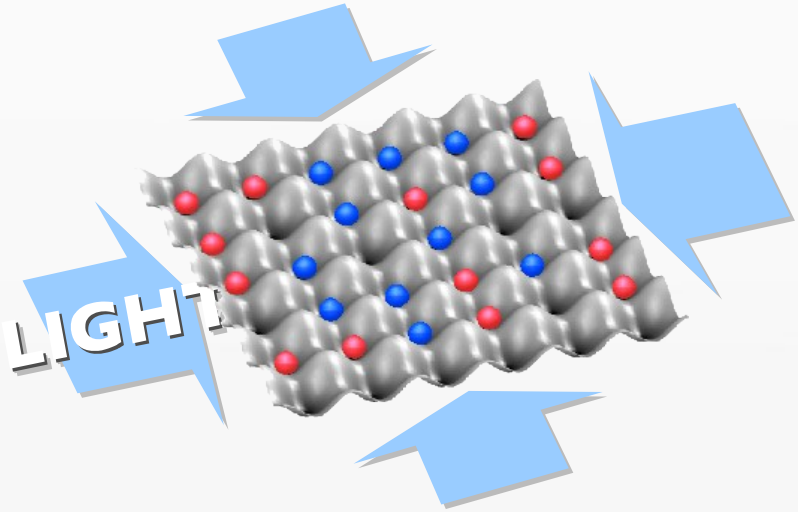


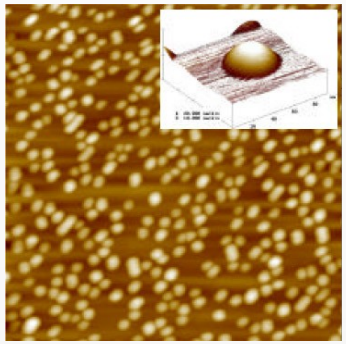




1	10	100	1000			10^{25}

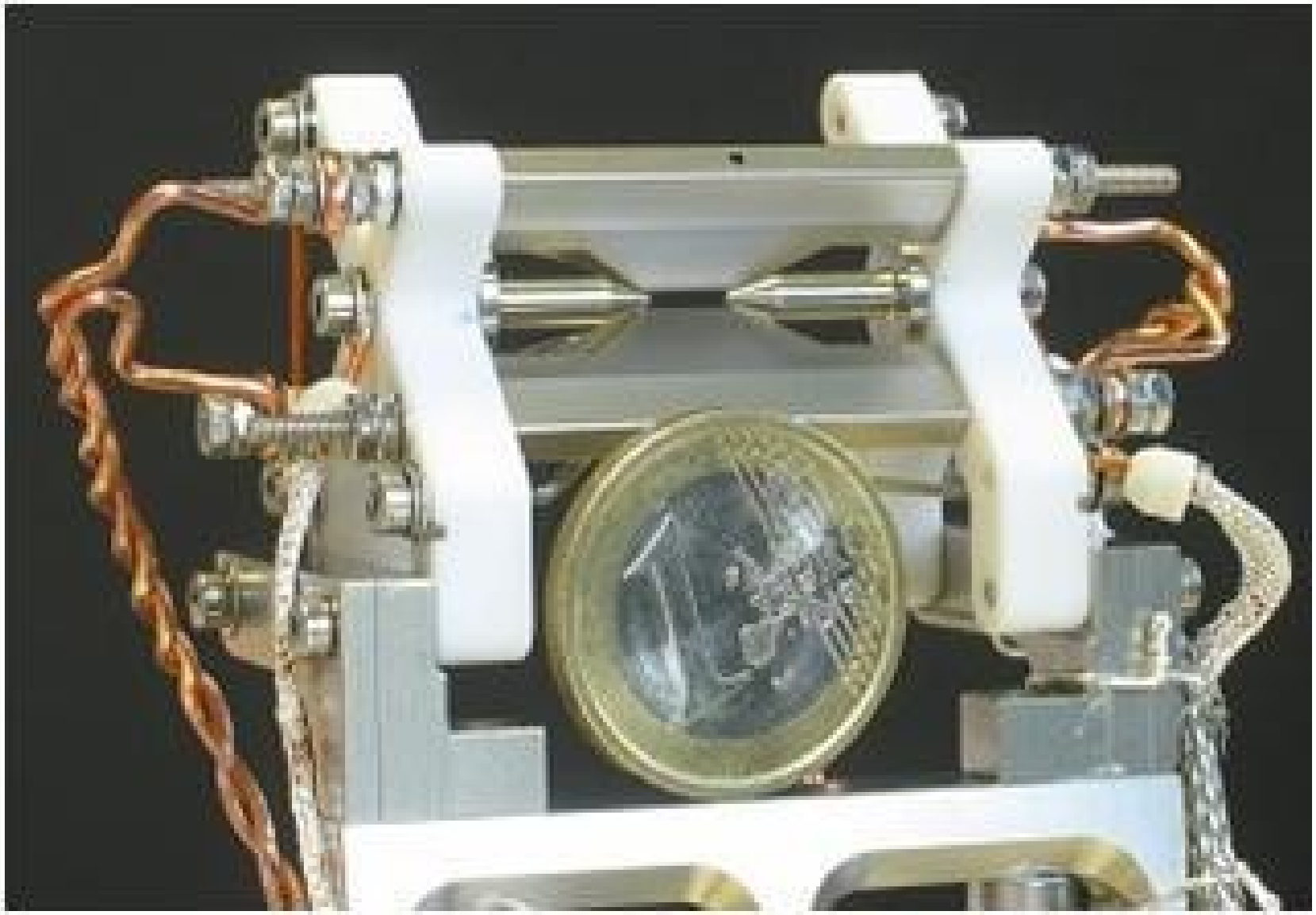




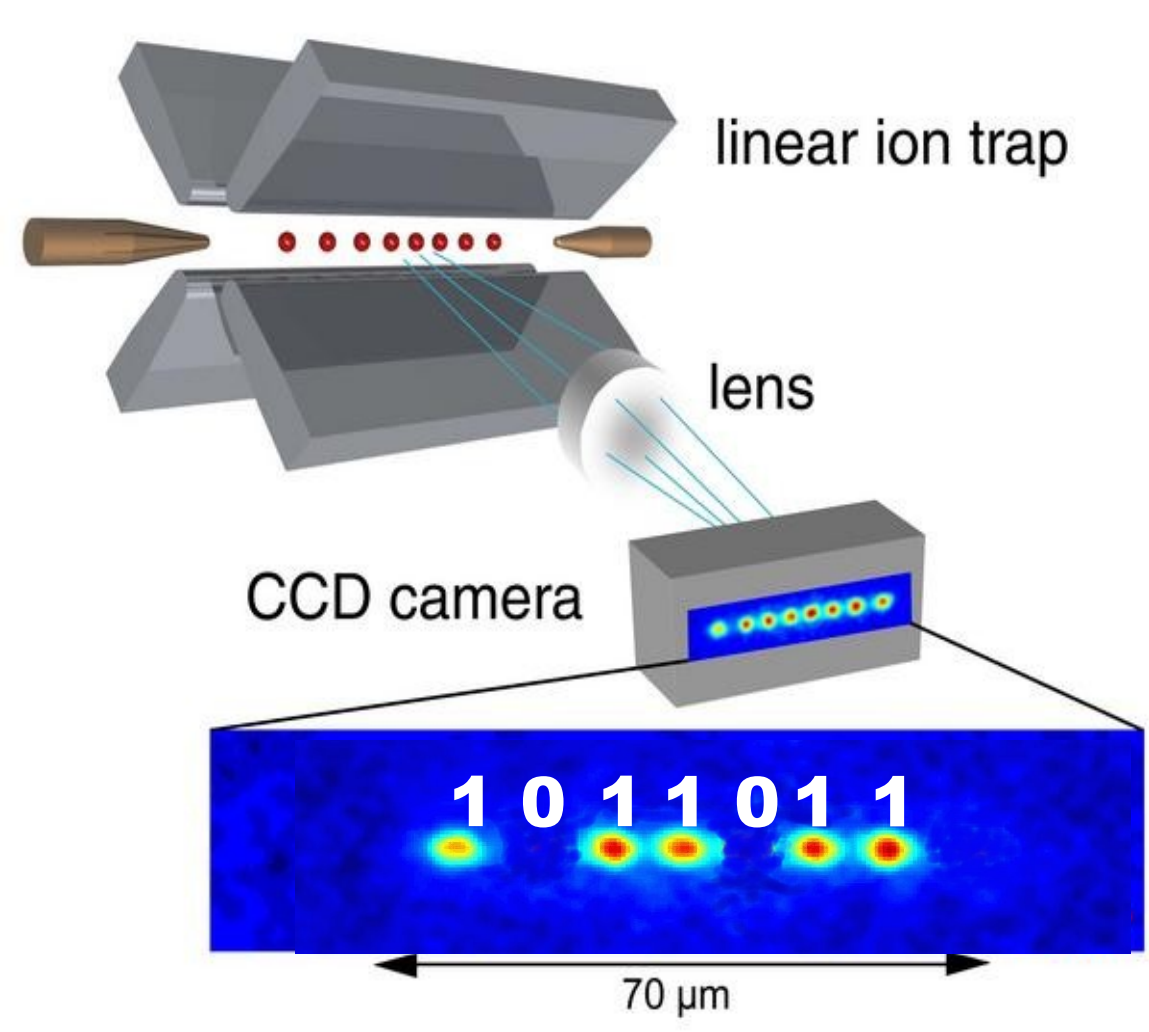


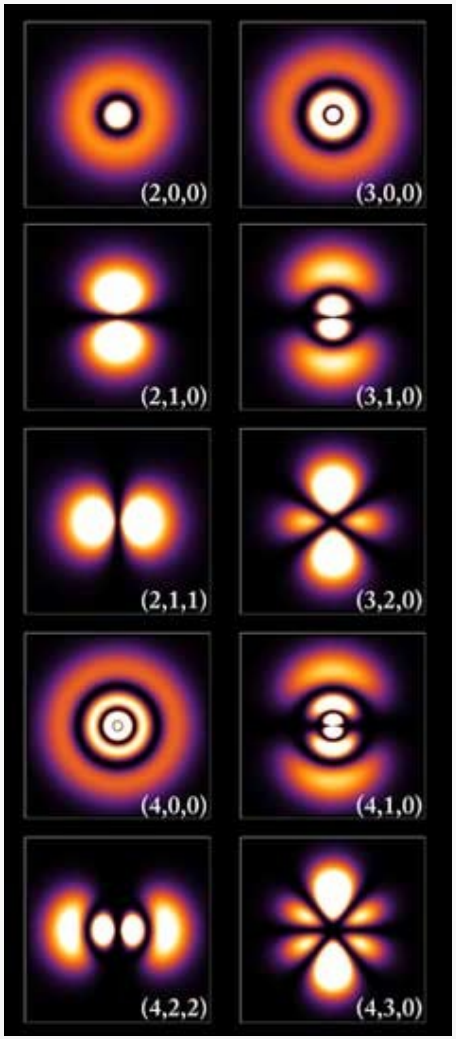
OTROS QUBITS

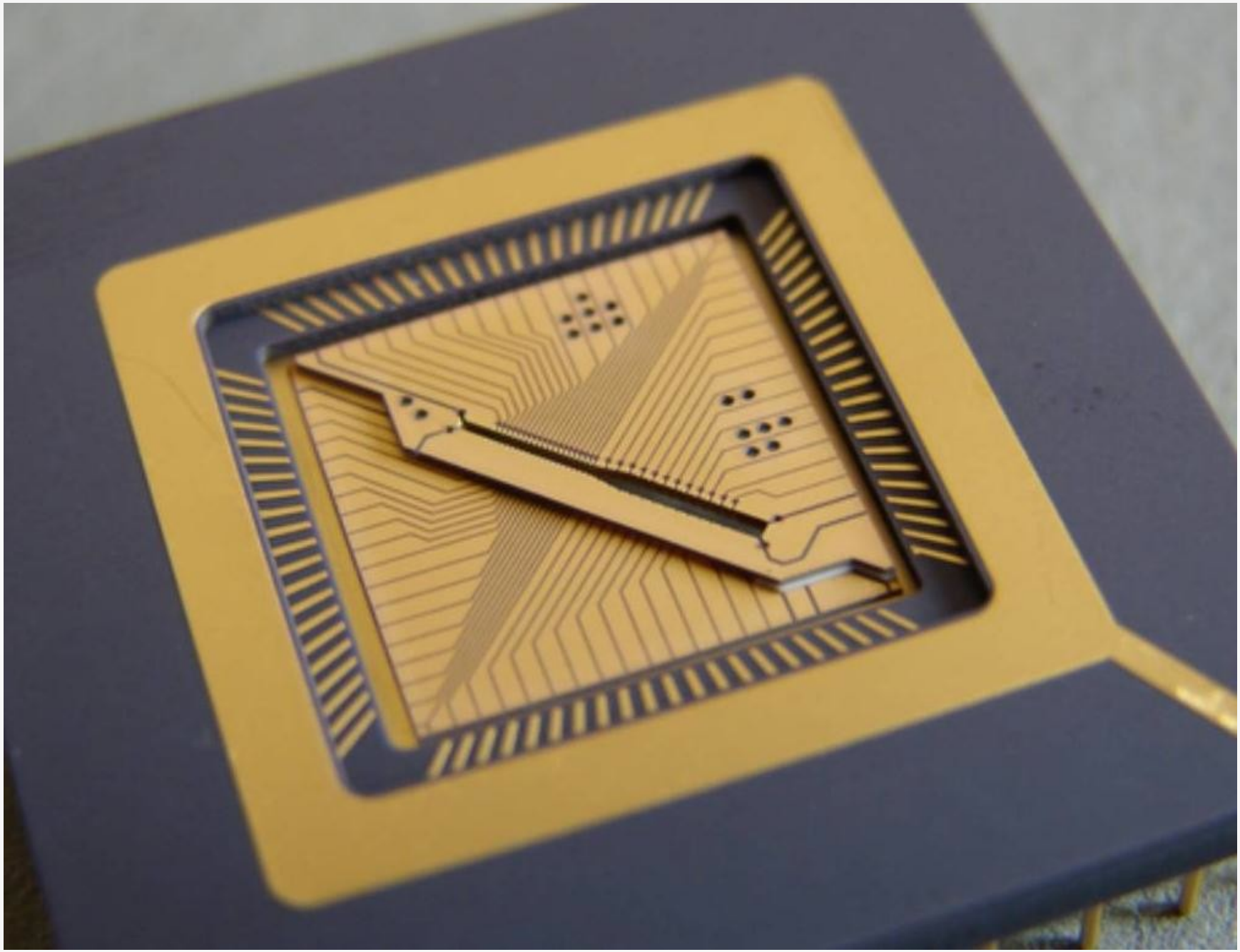
IONES



IONES


linear ion trap
lens
CCD camera
1 0 1 1 0 1 1
70 μm

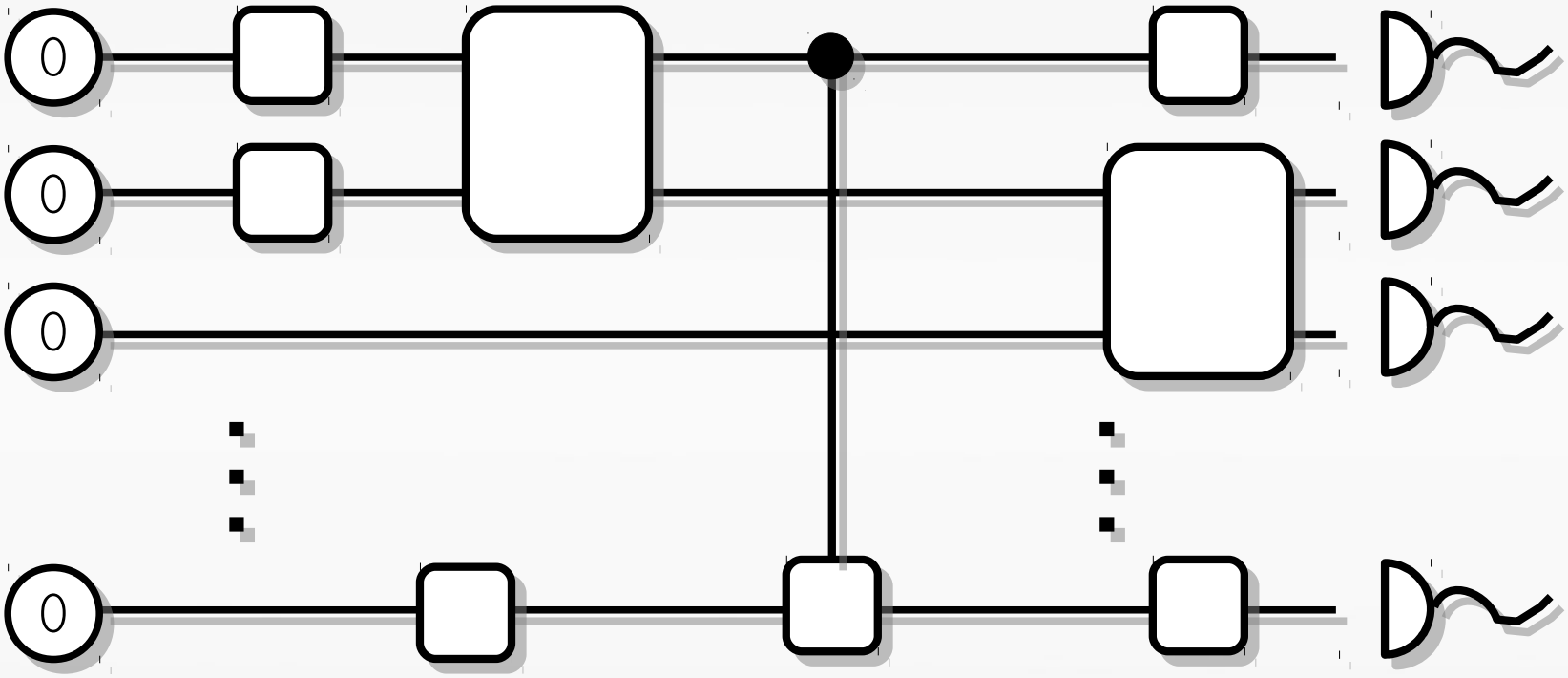

(2,0,0)
(3,0,0)
(2,1,0)
(3,1,0)
(2,1,1)
(3,2,0)
(4,0,0)
(4,1,0)
(4,2,2)
(4,3,0)



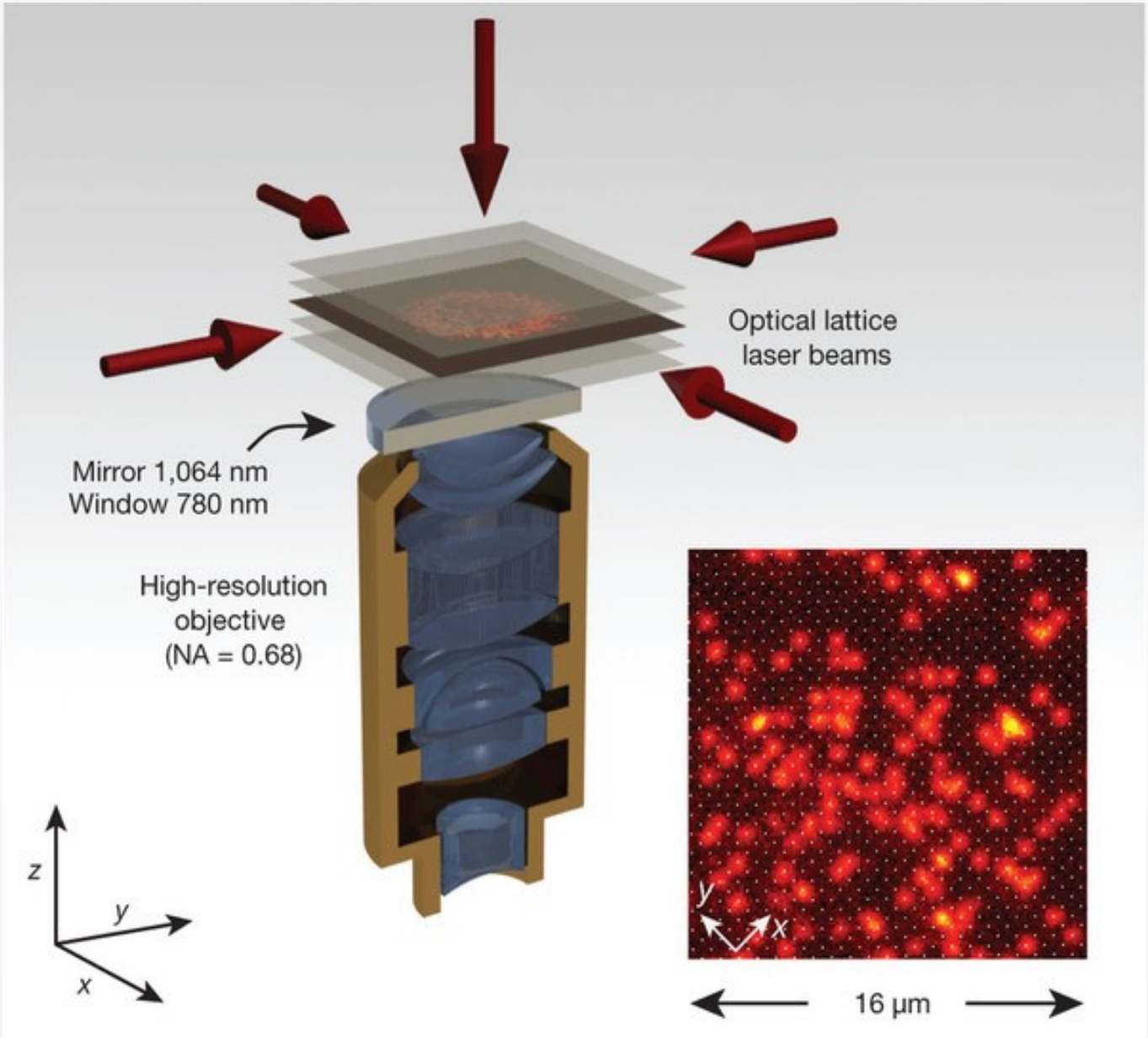
Pulsar aquí:

http://www.youtube.com/watch?v=OECq7epKHLE

OPERACIONES



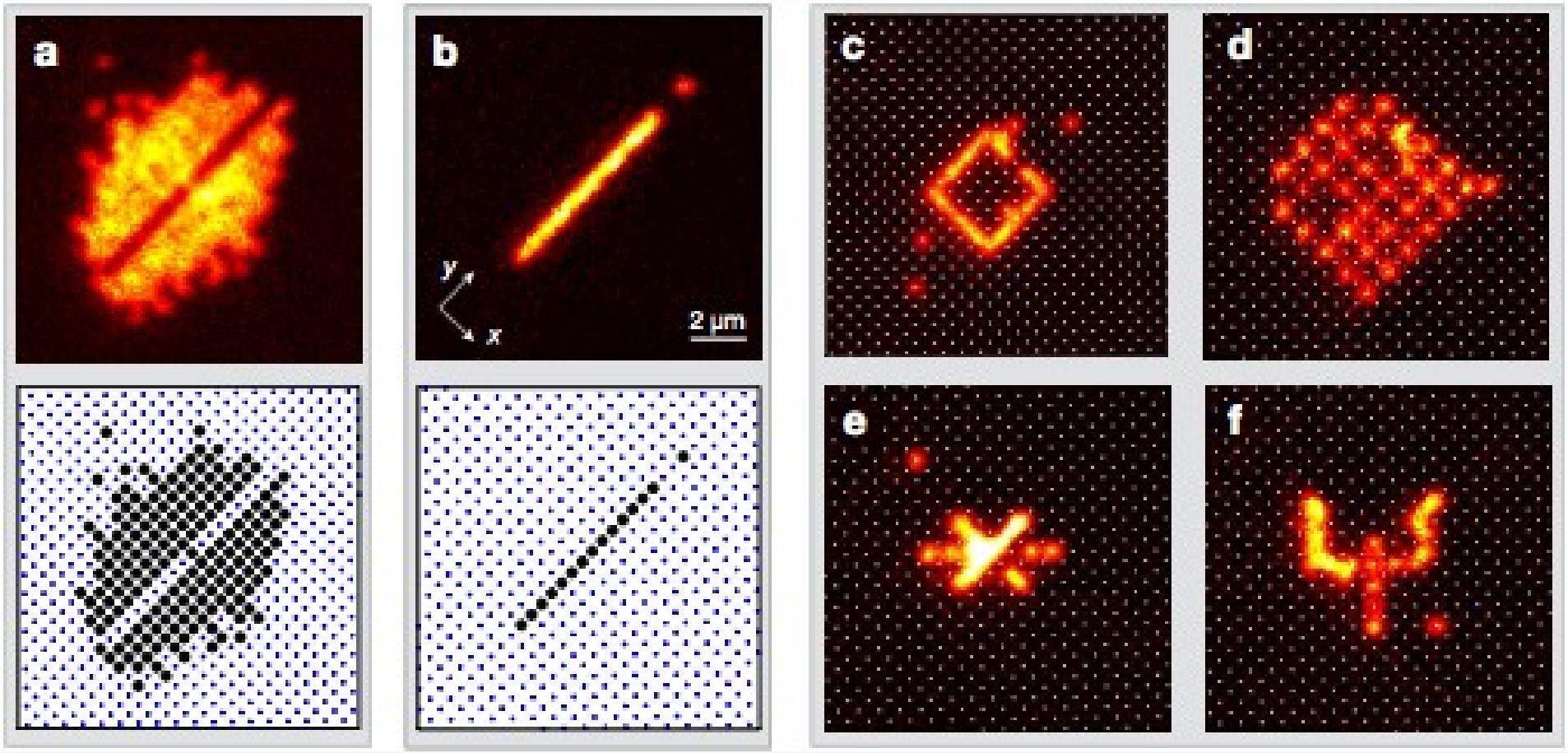
ÁTOMOS FRÍOS



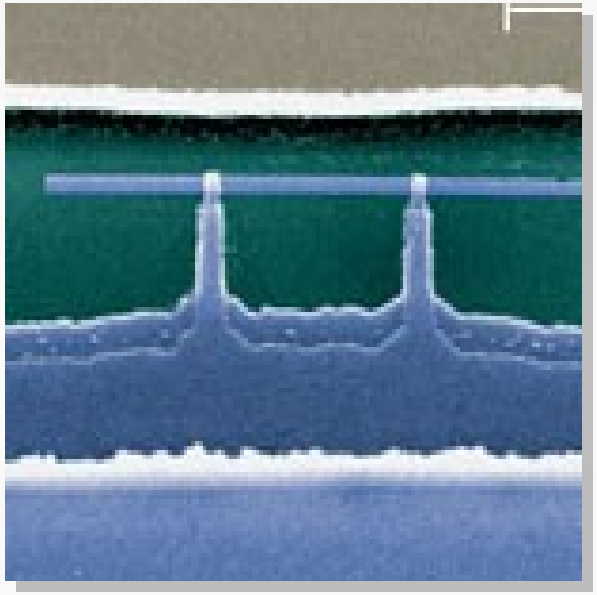
Pulsar aquí:

http://greiner.physics.harvard.edu/Videos/hopping.mpeg

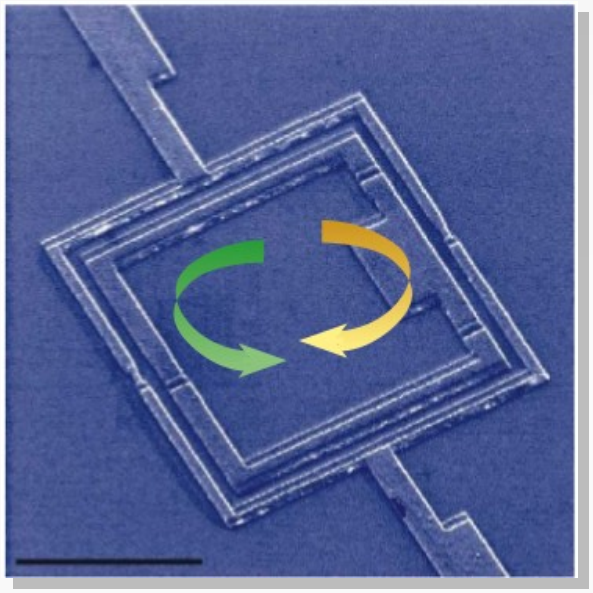
CONTROL



CIRCUITOS

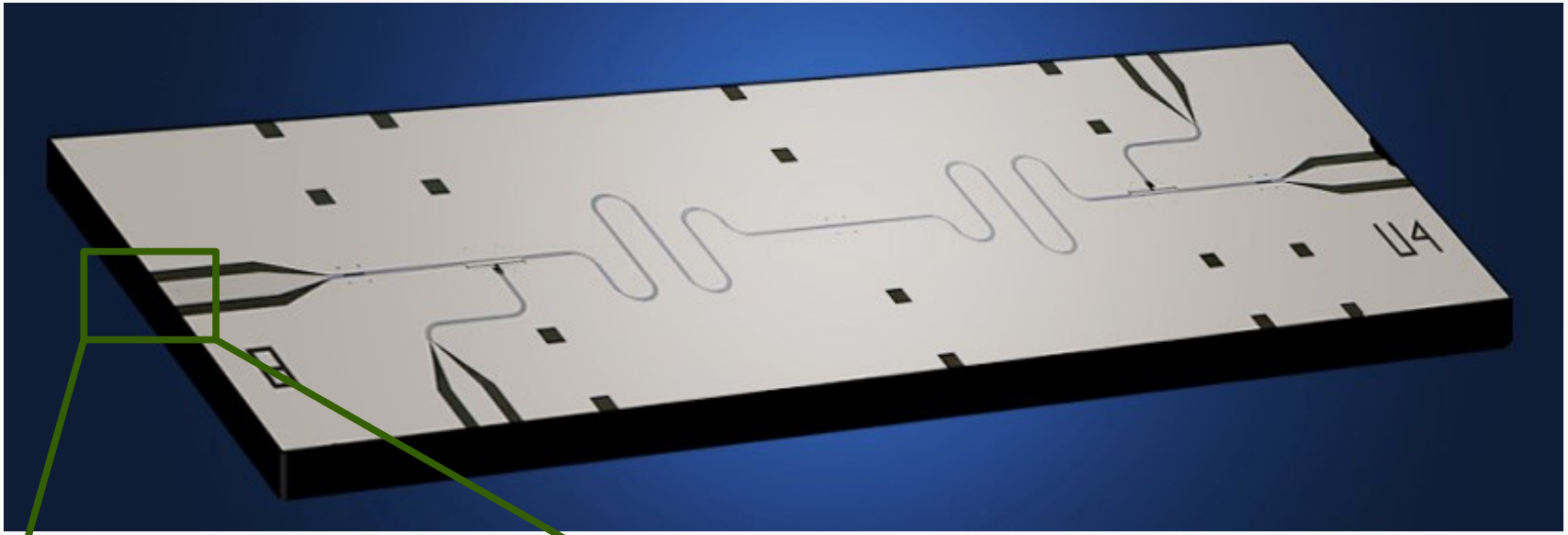


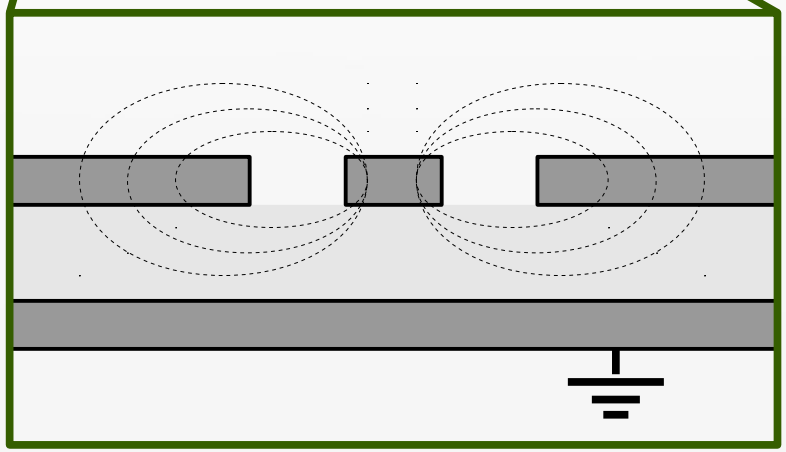
Qubit de carga



Qubit de flujo

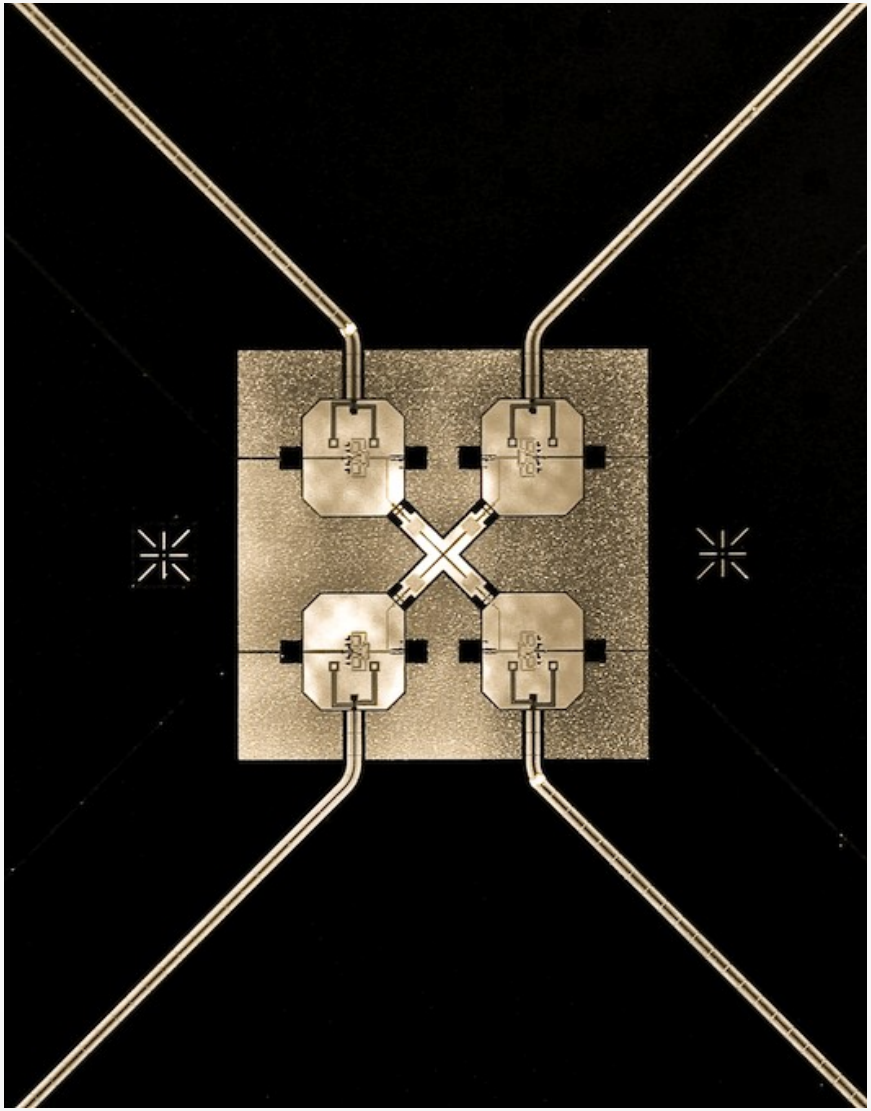
CIRCUITOS

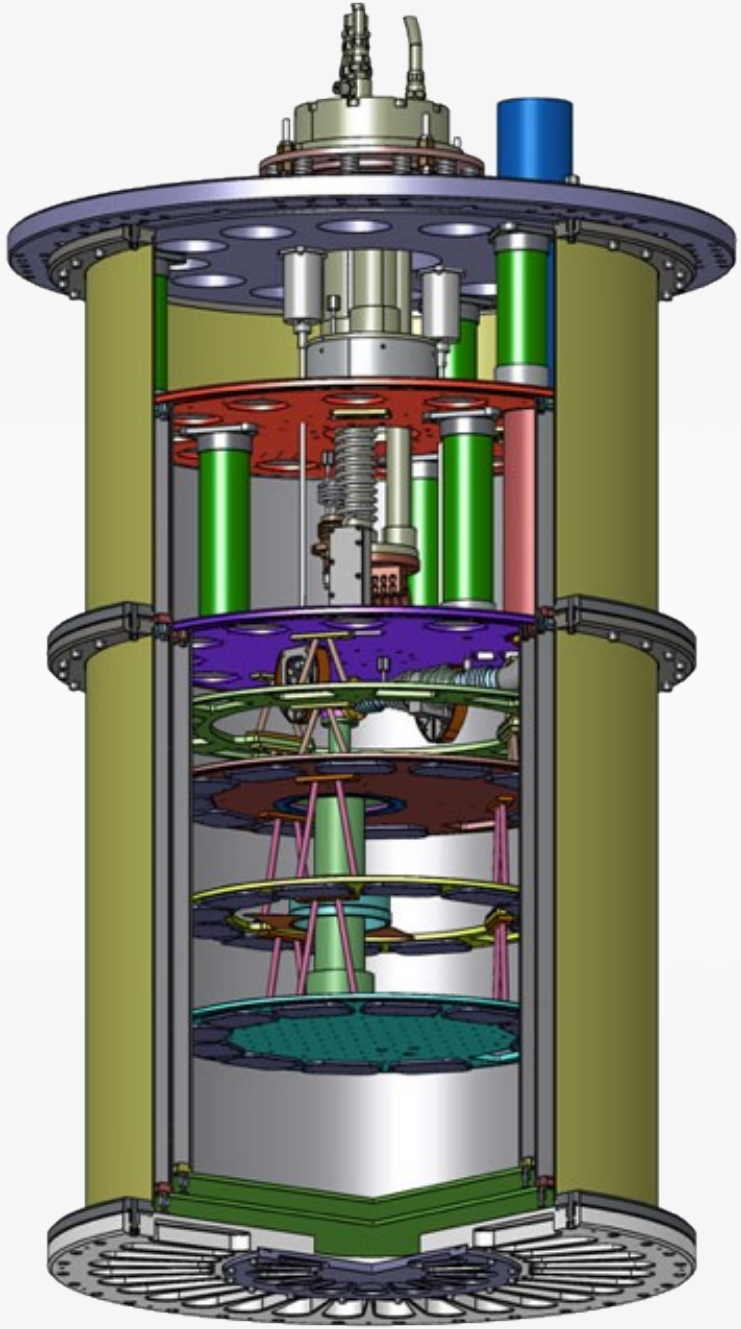




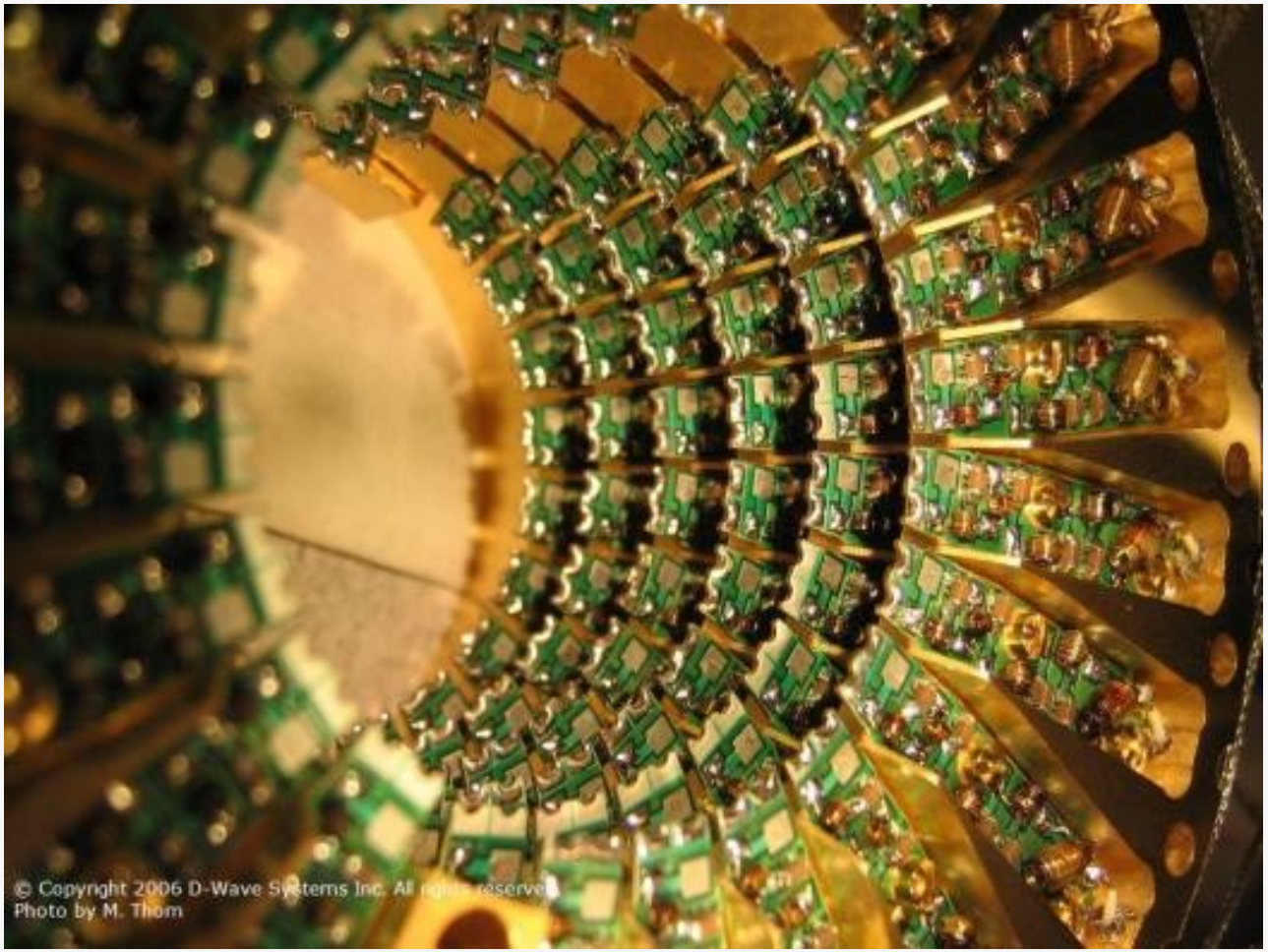
Guías de onda

- Transportan fotones de microondas.
- Permiten a los qubits interactuar entre sí.



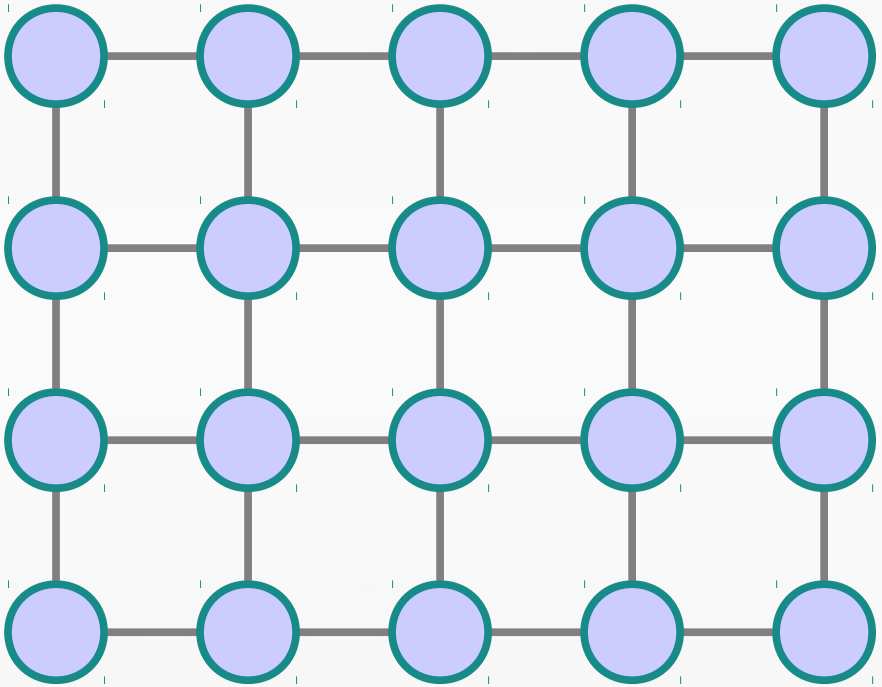


CIRCUITOS


© Copyright 2006 D-Wave Systems Inc. All rights reserved
Photo by M. Thom

Simulaciones clásicas

SIMULACIÓN CLÁSICA



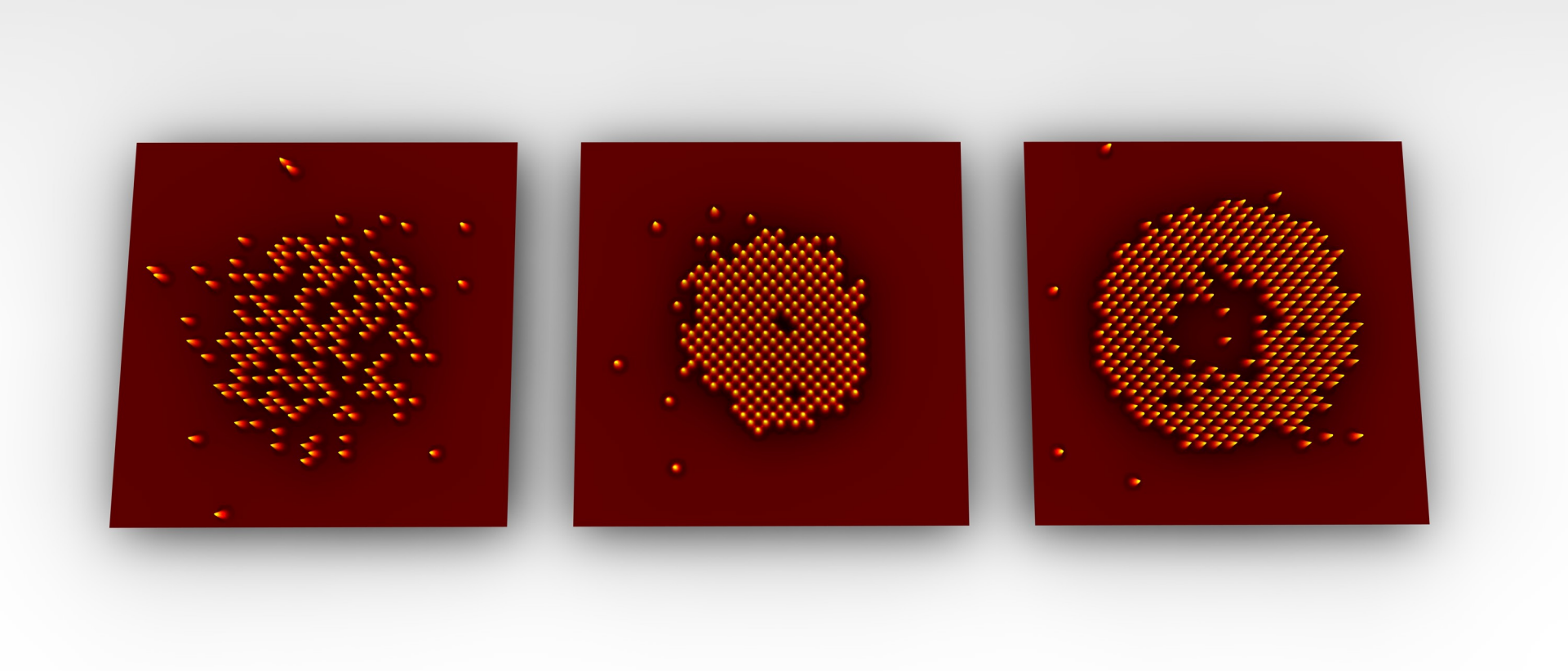
$$\sum_{ab\ldots z} c_{ab\ldots z} |a\, b \ldots\rangle$$

Exponentially large vector of numbers

$$c_{a\,b\ldots z} = F\left(A_a, A_b, \ldots A_z\right)$$

N times some complex object "A"

SIMULACIÓN CUÁNTICA



Simulate some quantum mechanical system with the same components of a quantum computer.