

Introducción a la Computación Cuántica

Primer Taller

**Luis Villaseñor
Profesor Visitante
CIIEC-BUAP
Profesor de Asignatura
ENES Morelia UNAM**

29/Noviembre/2022

Contenido del Primer Taller

1. Introducción a la Mecánica Cuántica

1.1 Superposición de Estados Cuánticos

1.2 Entrelazamiento Cuántico

1.3 Interferencia y Medición

2. Introducción a la Computación Cuántica

2.1 Superposición con 1 Qubit

2.2 Superposición con 2 Qubits

2.3 Computación Cuántica vs Clásica

2.4 Implementación de los Qubits

2.5 Ejemplos de Tecnologías

3. Compuertas Cuánticas

4. Introducción a Python y a la Programación Cuántica con Qiskit

5. Parte Práctica del Primer Taller

5.1 Brevísima Introducción a Python

5.2. Introducción a la Programación Cuántica usando Qiskit

5.2.1 Compuertas Cuánticas

5.2.2 Un Primer Circuito Cuántico Arbitrario

5.2.3 Circuito Cuántico para Superposición Simétrica

5.2.4 Entrelazamiento de 2 Qubits. Estados de Bell

5.2.5 Entrelazamiento de 3 Qubits. Estados GHZ

5.2.6 Teleportación Cuántica

5.2.6.1 Sustento Matemático del Protocolo de Teleportación Cuántica

Segundo Taller

Algoritmos Cuánticos

Tercer Taller

Machine Learning con Computación Cuántica

Parte Práctica con Jupyter Notebook en Google Colab

En el siguiente link podrán descargar el material del taller

<https://github.com/lvillasen/Introduccion-a-la-Computacion-Cuantica>

1. Mecánica Cuántica

Rama de la Física que explica la materia y la energía a nivel atómico y sub-atómico.

Surgió en las primeras 3 décadas del siglo pasado

La materia, la energía, el momento angular, la carga, el momento lineal de las partículas sub-atómicas están cuantizados

Cuanto de Energía de Planck para un Fotón

$$E = h\nu$$

$$h = 6.6262 \times 10^{-34} \text{ J}\cdot\text{s}$$

v = frequency (Hz)

Longitud de Onda de de Broglie

$$\lambda = \frac{h}{mv} = \frac{h}{p}$$

Ecuación de Schrodinger

$$\left[\frac{-\hbar^2}{2m} \nabla^2 + V \right] \Psi = i\hbar \frac{\partial}{\partial t} \Psi$$

Para una partícula libre

$$\psi(\mathbf{r}, t) = Ae^{i(\mathbf{k}\cdot\mathbf{r}-\omega t)} = Ae^{i(\mathbf{p}\cdot\mathbf{r}-Et)/\hbar}$$

Reunión Solvay de 1927



Interpretación de la Función de Onda

$$\rho(\mathbf{r}, t) = \psi^*(\mathbf{r}, t)\psi(\mathbf{r}, t) = |\psi(\mathbf{r}, t)|^2$$

Condición de Normalización

$$\int_{\text{all space}} |\psi(\mathbf{r}, t)|^2 d^3\mathbf{r} = 1$$

1.1 Mecánica Cuántica. Superposición de Estados

Para un sistema cuántico de 2 estados

Ket

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

alfa y beta son números complejos

Bra

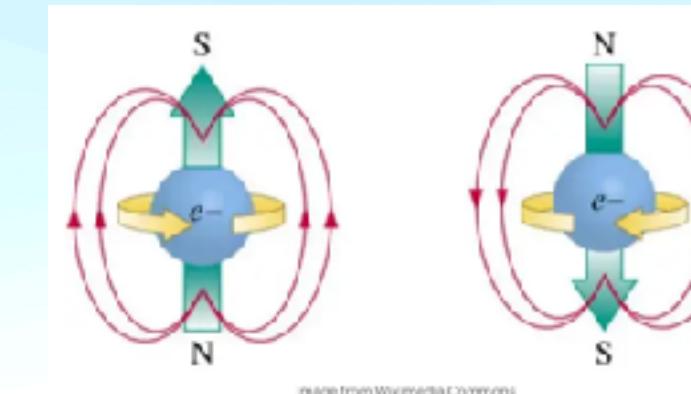
$$\langle\Psi| = \alpha^*\langle 0| + \beta^*\langle 1|$$

Al medir $|\psi\rangle$ siempre se obtiene $|0\rangle$ o $|1\rangle$
(colapso de la función de onda)

Condición de normalización

$$|\alpha|^2 + |\beta|^2 = 1$$

Ejemplo de un sistema de 2 estados es el espín del electrón

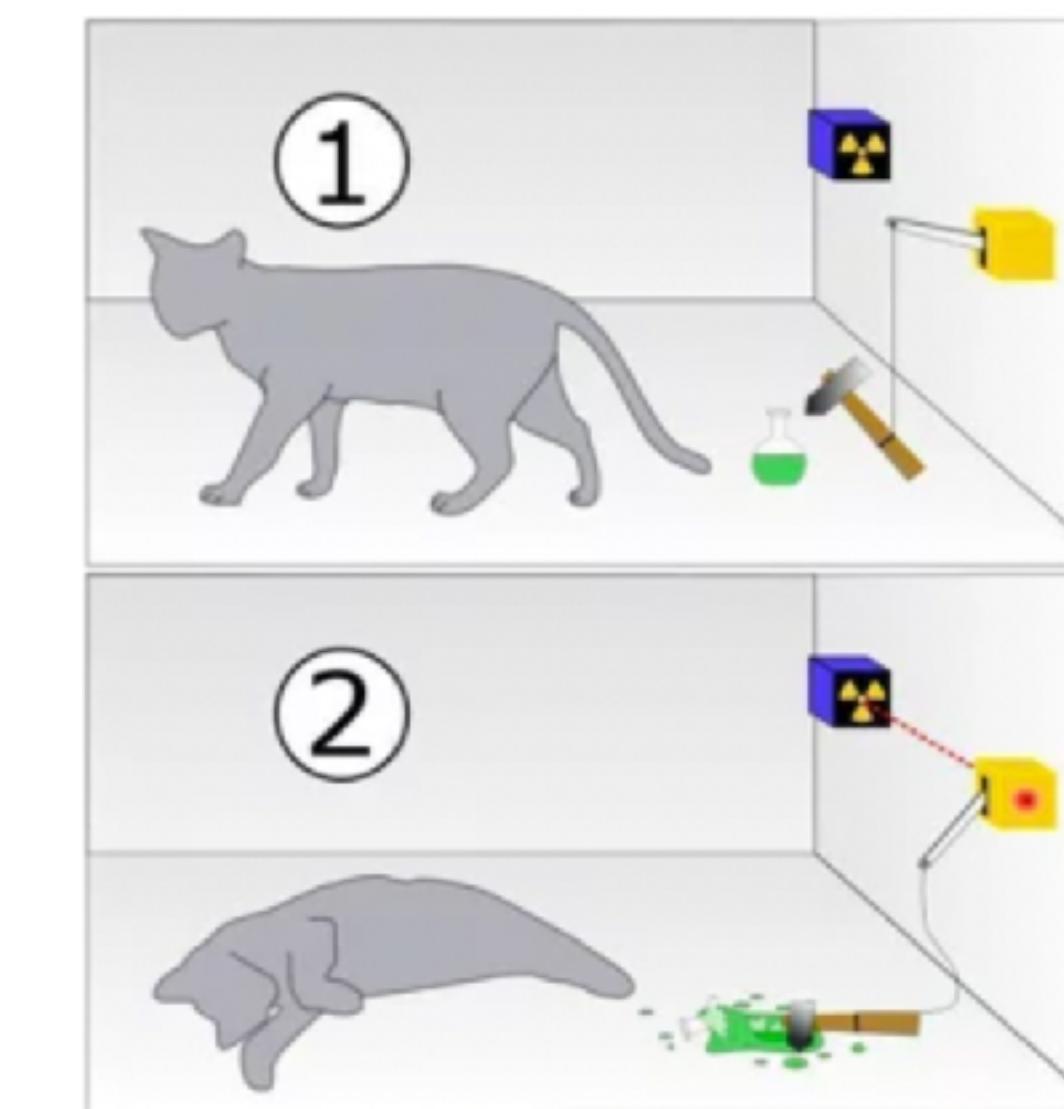


Representación matricial

$$\text{Ket } |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\text{Bra } \langle 0| := (1 \ 0)$$

$$|\Psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$



$$|\text{cat}\rangle = \alpha \left| \begin{array}{c} \text{cat} \\ \text{alive} \end{array} \right\rangle + \beta \left| \begin{array}{c} \text{cat} \\ \text{dead} \end{array} \right\rangle$$

Producto Tensorial

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

$$|\Phi\rangle = \gamma|0\rangle + \delta|1\rangle$$

$$|\Psi\rangle|\Phi\rangle = |\Psi\rangle \otimes |\Phi\rangle = |\Psi\Phi\rangle$$

$$\begin{aligned} |\Psi\Phi\rangle &= (\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle) \\ &= \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle \end{aligned}$$

1.1 Mecánica Cuántica. Superposición de Estados

Para un sistema cuántico de 4 estados. Por ejemplo un sistema compuesto de dos subsistemas de 2 estados cada uno

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

Representación matricial

La medición de este sistema tiene 2^2 resultados posibles y se representa como la superposición de esos 4 estados base

$$|00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, |01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, |10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \text{ and } |11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

Condición de normalización

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1.$$

$$|a\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle = \begin{bmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{bmatrix}$$

En general un sistema cuántico compuesto por n subsistemas de 2 estados c/u se representa como la superposición de 2^n estados base.

Una medicación

colapsa su función de onda a uno de esos estados base

1.2 Mecánica Cuántica. Entrelazamiento Cuántico

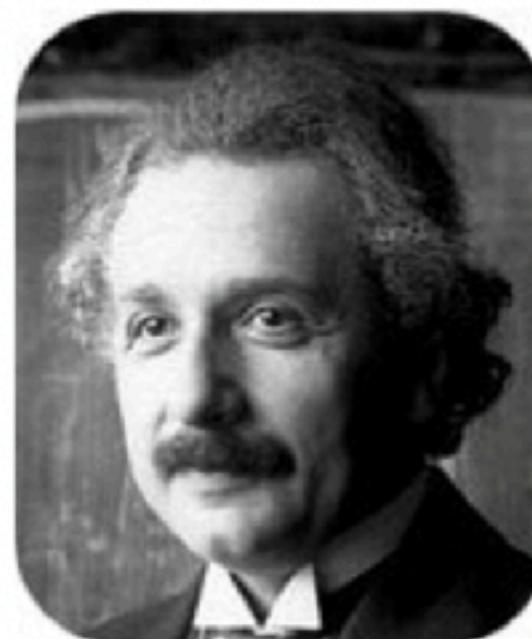
Dos partículas o dos qubits están entrelazados cuando la medición de uno determina instantáneamente el estado cuántico del otro sin importar a qué distancia estén entre si.

Estados de Bell

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$$

$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$$

Paradoja EPR en 1935



A. Einstein



B. Podolsky



N. Rosen

Los estados factorizables NO están entrelazados

Producto Tensorial

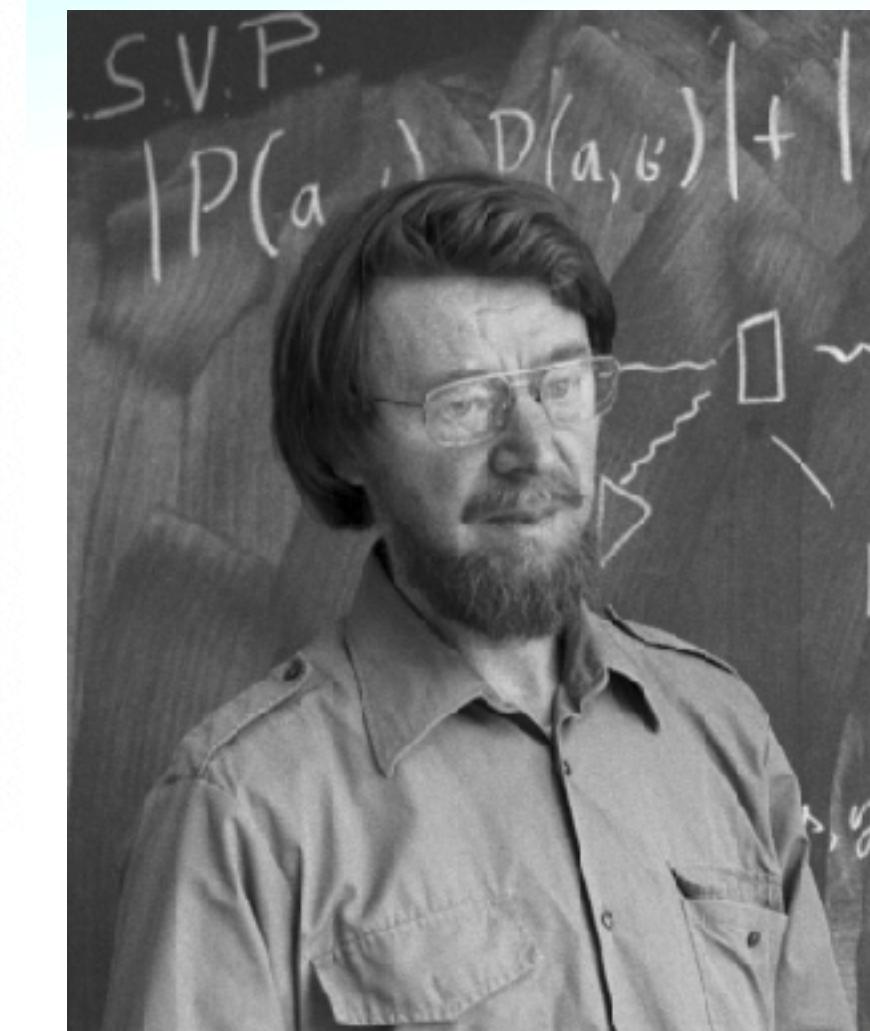
$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$|\Phi\rangle = \gamma|0\rangle + \delta|1\rangle$$

$$|\Psi\rangle|\Phi\rangle = |\Psi\rangle \otimes |\Phi\rangle = |\Psi\Phi\rangle$$

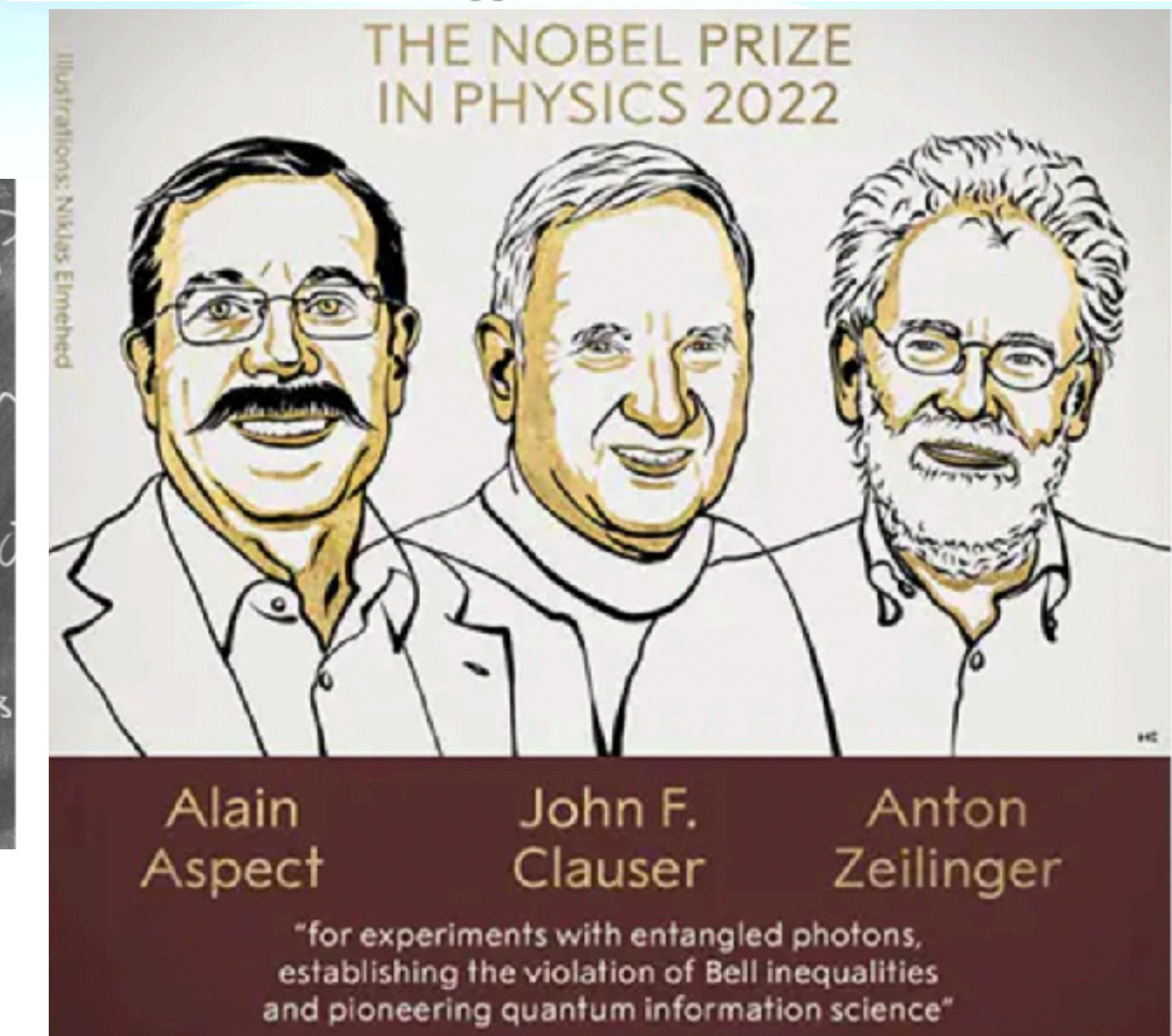
$$\begin{aligned} |\Psi\Phi\rangle &= (\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle) \\ &= \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle \end{aligned}$$

Desigualdad de Bell en 1964



Ejemplo de Estados Entrelazados que no son Estados de Bell

$$|\psi\rangle = \cos(\theta)|00\rangle + \sin(\theta)|11\rangle$$

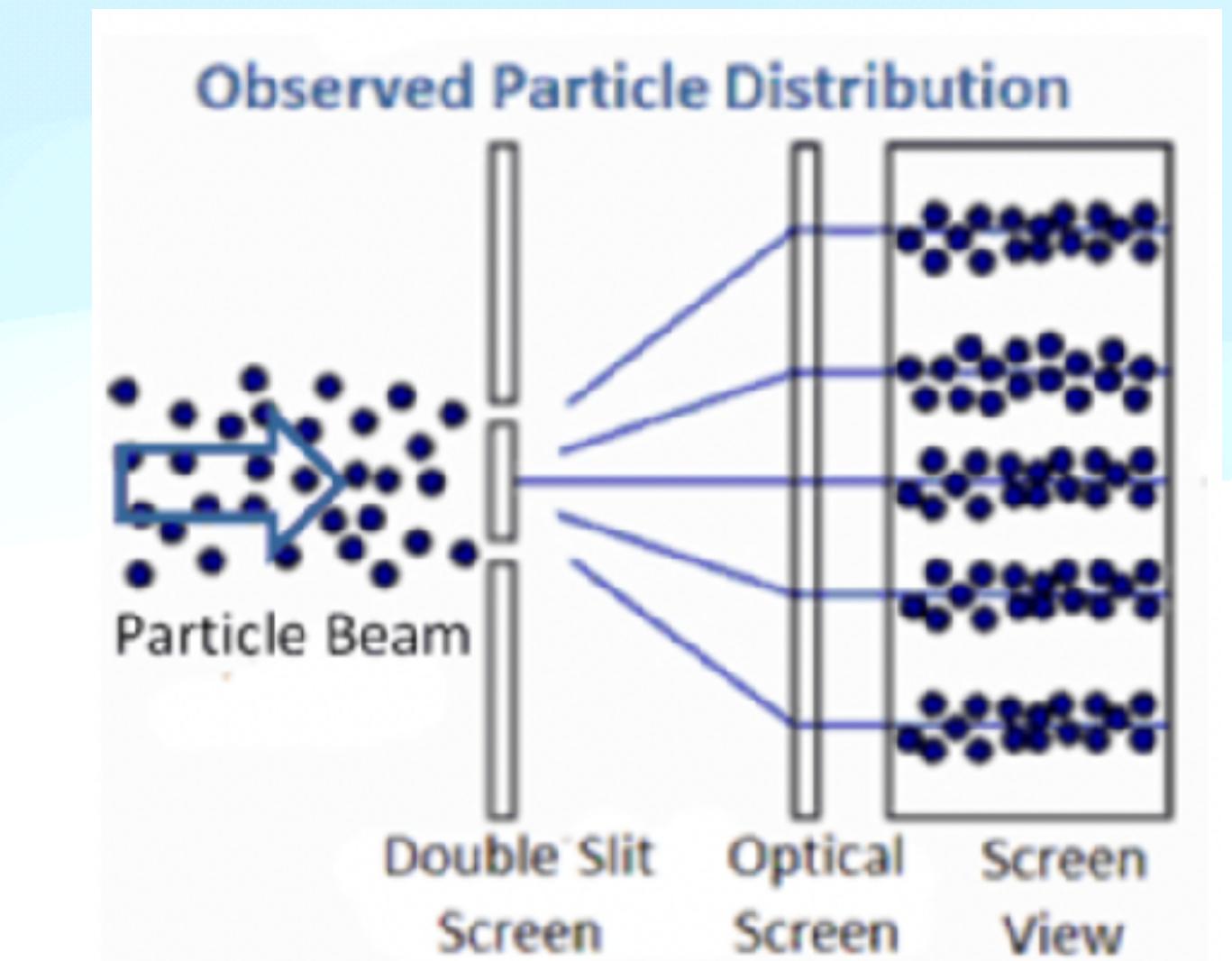
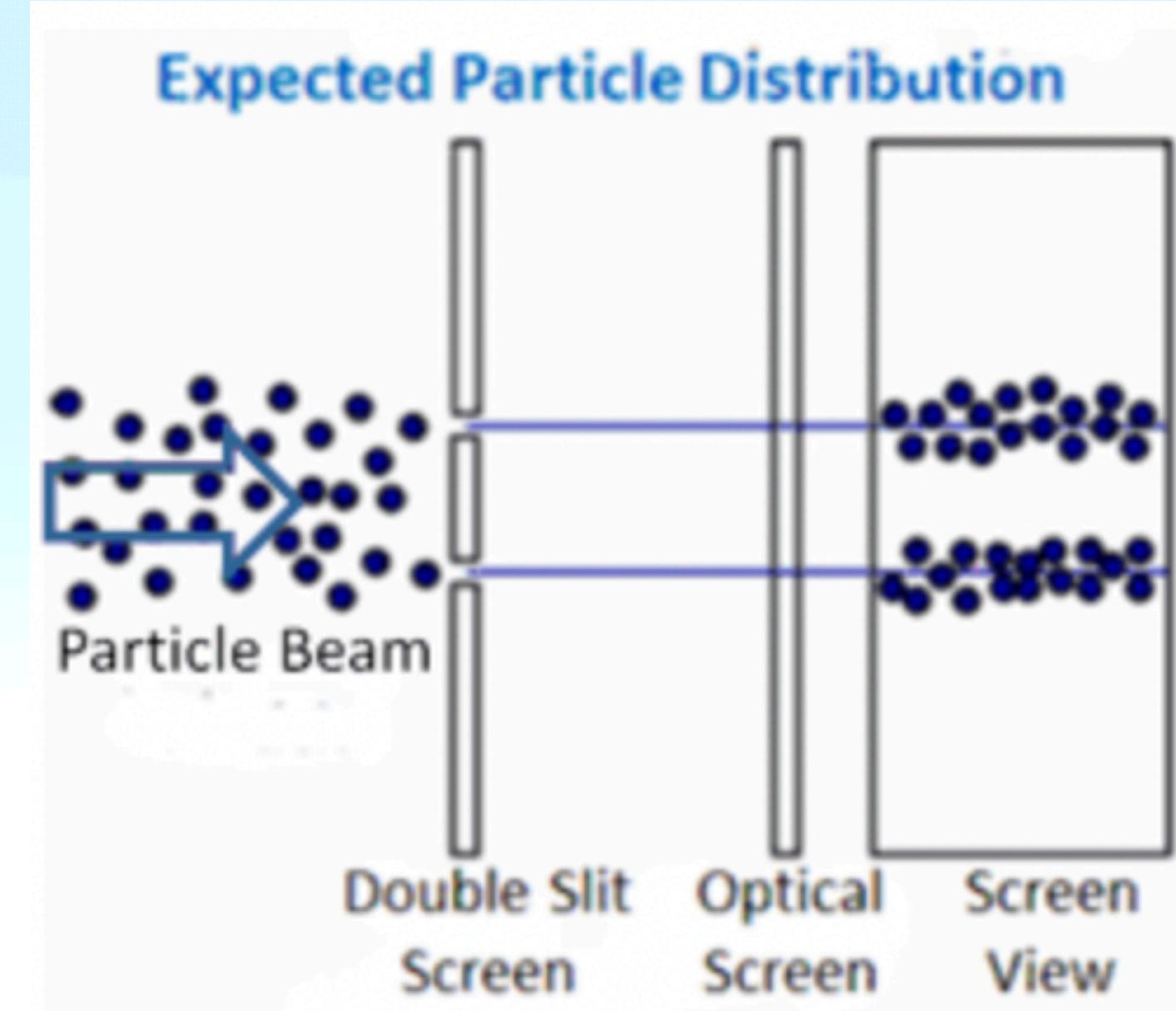
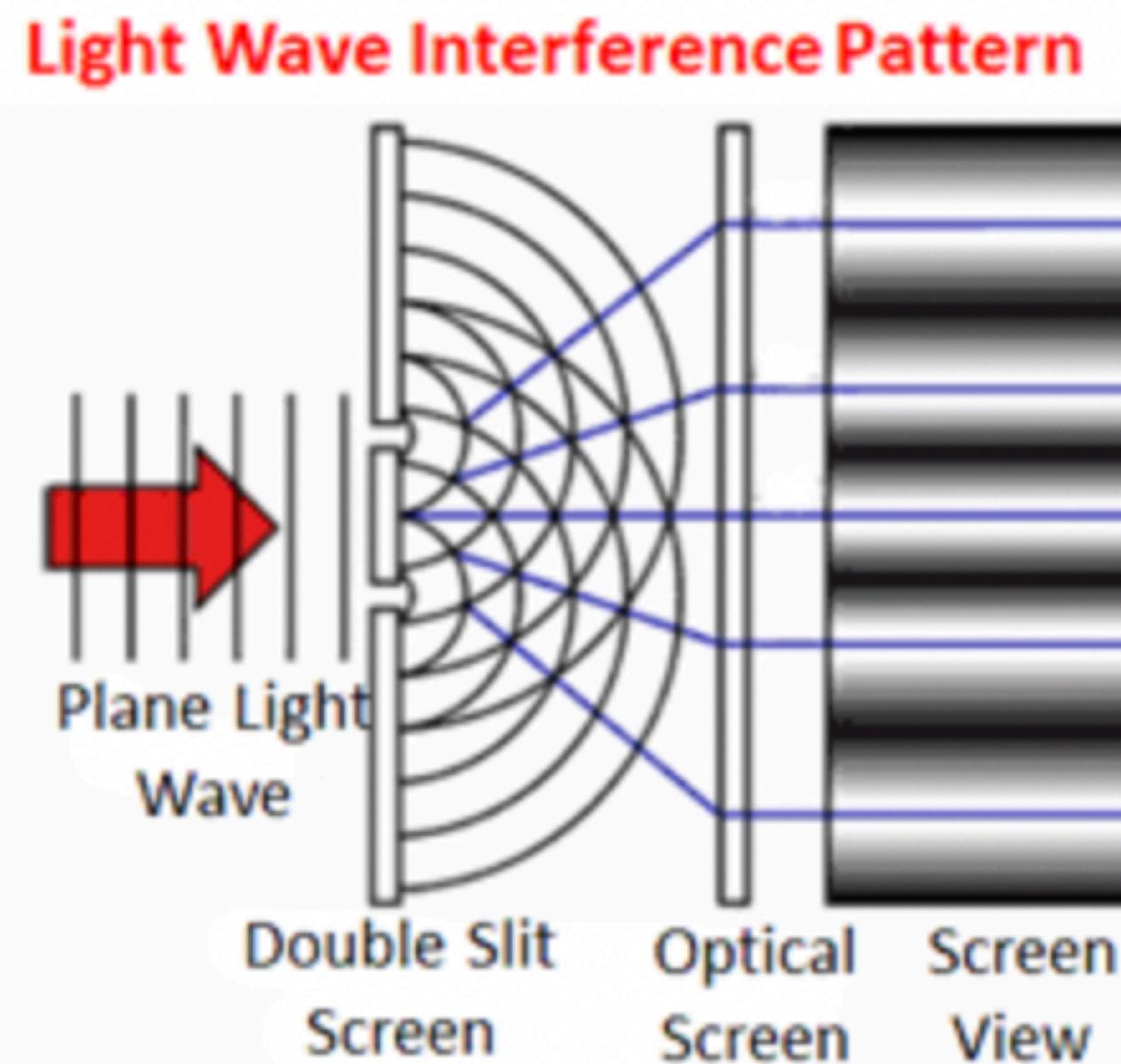


1.3 Mecánica Cuántica. Interferencia y Medición

1801 Thomas Young

Lo que se esperaría clásicamente para partículas

Lo que se observa. Las partículas interfieren como ondas pero se Observan como partículas



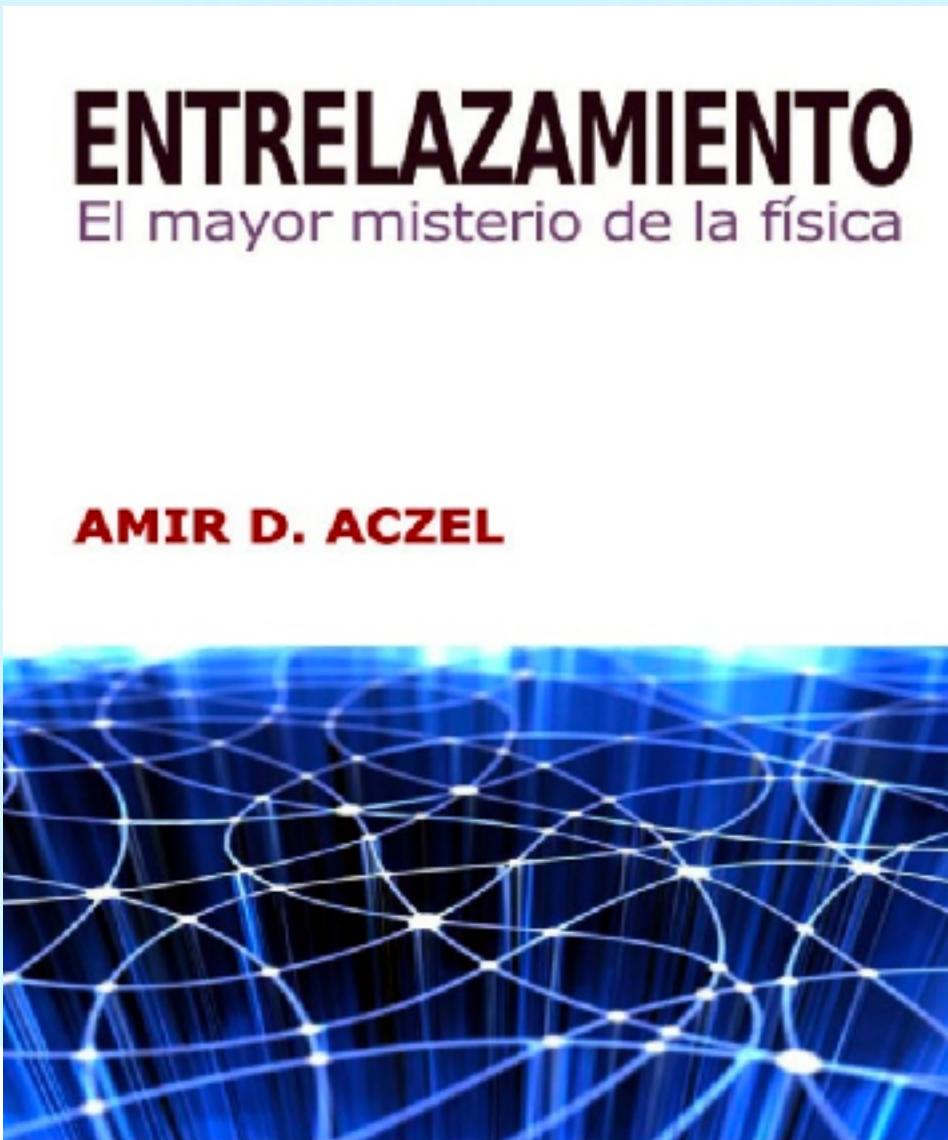
Images Public Domain: by Inductiveload, Modified

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

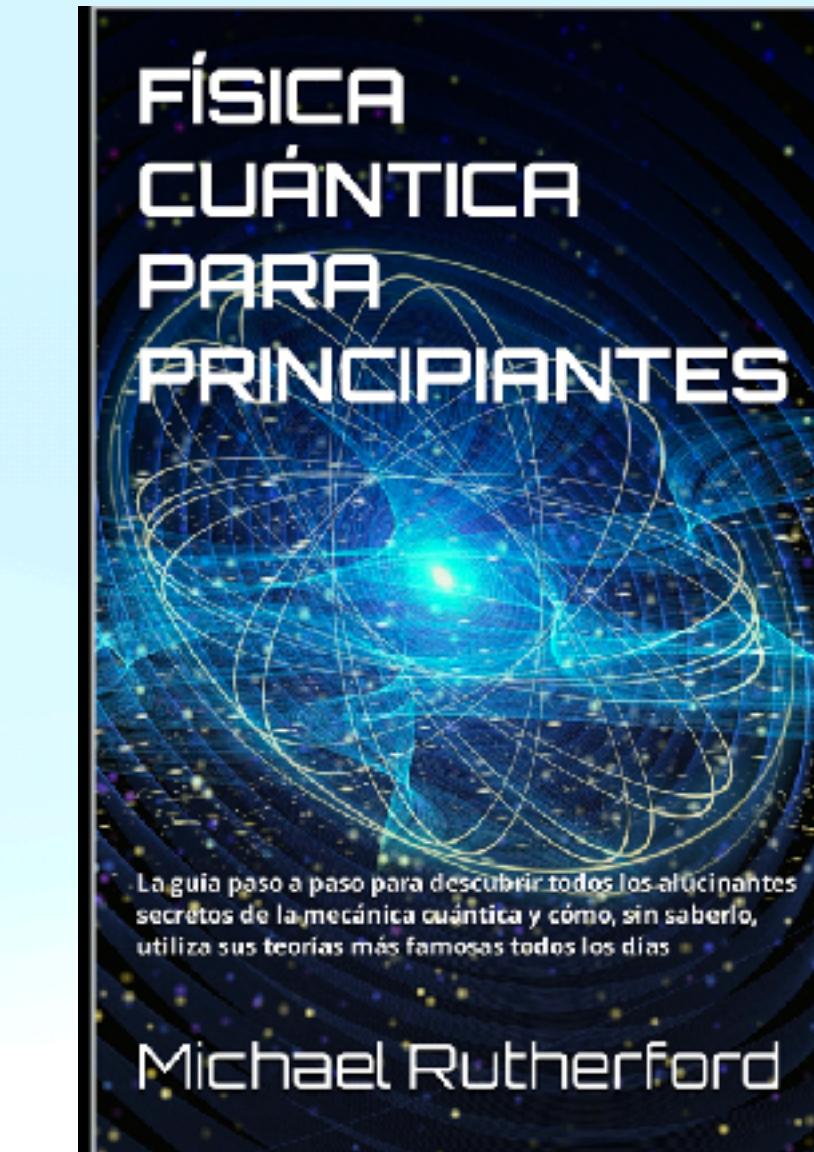
Al medir $|\psi\rangle$ siempre se obtiene $|0\rangle$ o $|1\rangle$
(colapso de la función de onda)

Para saber más sobre Mecánica Cuántica

<http://www.librosmaravillosos.com/>



2004



Premio Nobel de Física 2022, La contribución y sus implicaciones
José Luis Lucio. CIEC-BUAP

<https://www.facebook.com/CiiecBuap/videos/1195263281058560/>

2. Introducción a la Computación Cuántica

Nueva manera de hacer cómputo usando las leyes de la mecánica cuántica para resolver problemas demasiado complejos para las computadoras tradicionales a través de la Superposición, el Entrelazamiento y la Interferencia Cuántica

Hay varios modelos de computación cuántica: Circuitos Cuánticos, máquina de Turing Cuántica, Recocido (Annealing) Cuántico y Computación Cuántica Adiabática.

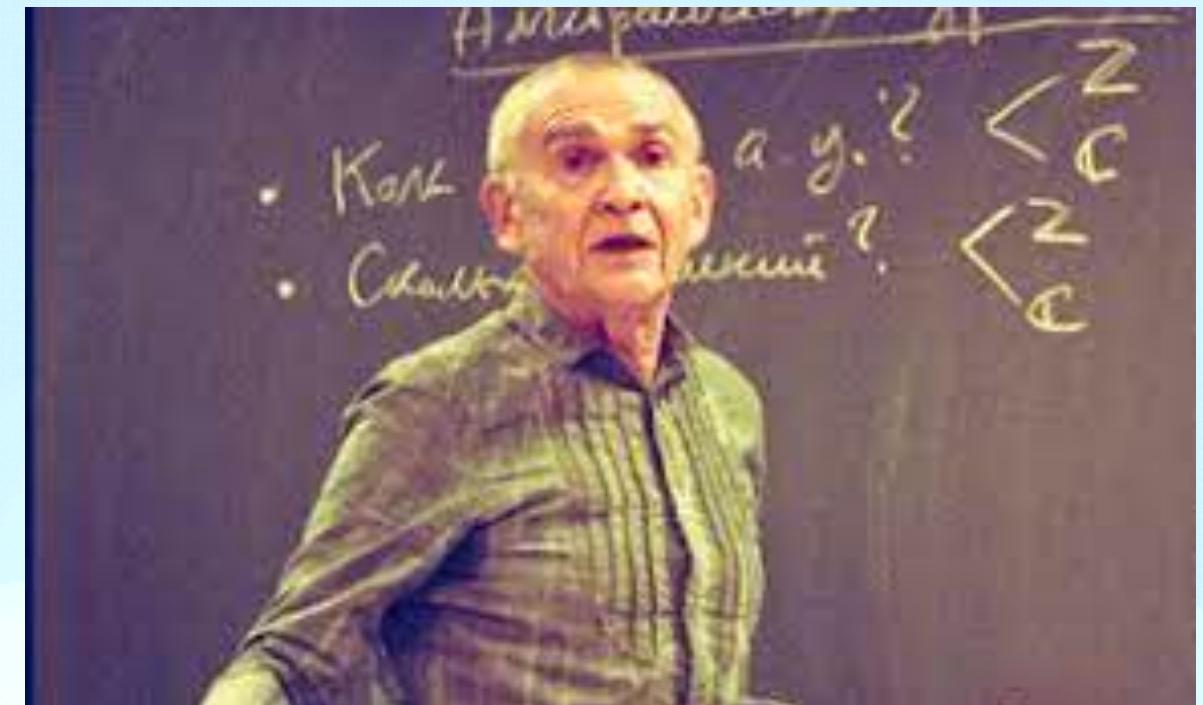
Veremos Circuitos Cuánticos en detalle.

Richard Feynman en 1981



Physics of Computation Conference Endicott House MIT May 6-8, 1981

Matemático Russo Yuri Manin en 1980



Algoritmo de Factorización de Shor en 1994



2.1 Computación Cuántica. Superposición con 1 Qubit

Un qubit es un sistema cuántico con dos estados

descrito por la superposición de los 2 estados

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad |\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$|\alpha|^2 + |\beta|^2 = 1 \quad |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

alfa y beta son números complejos

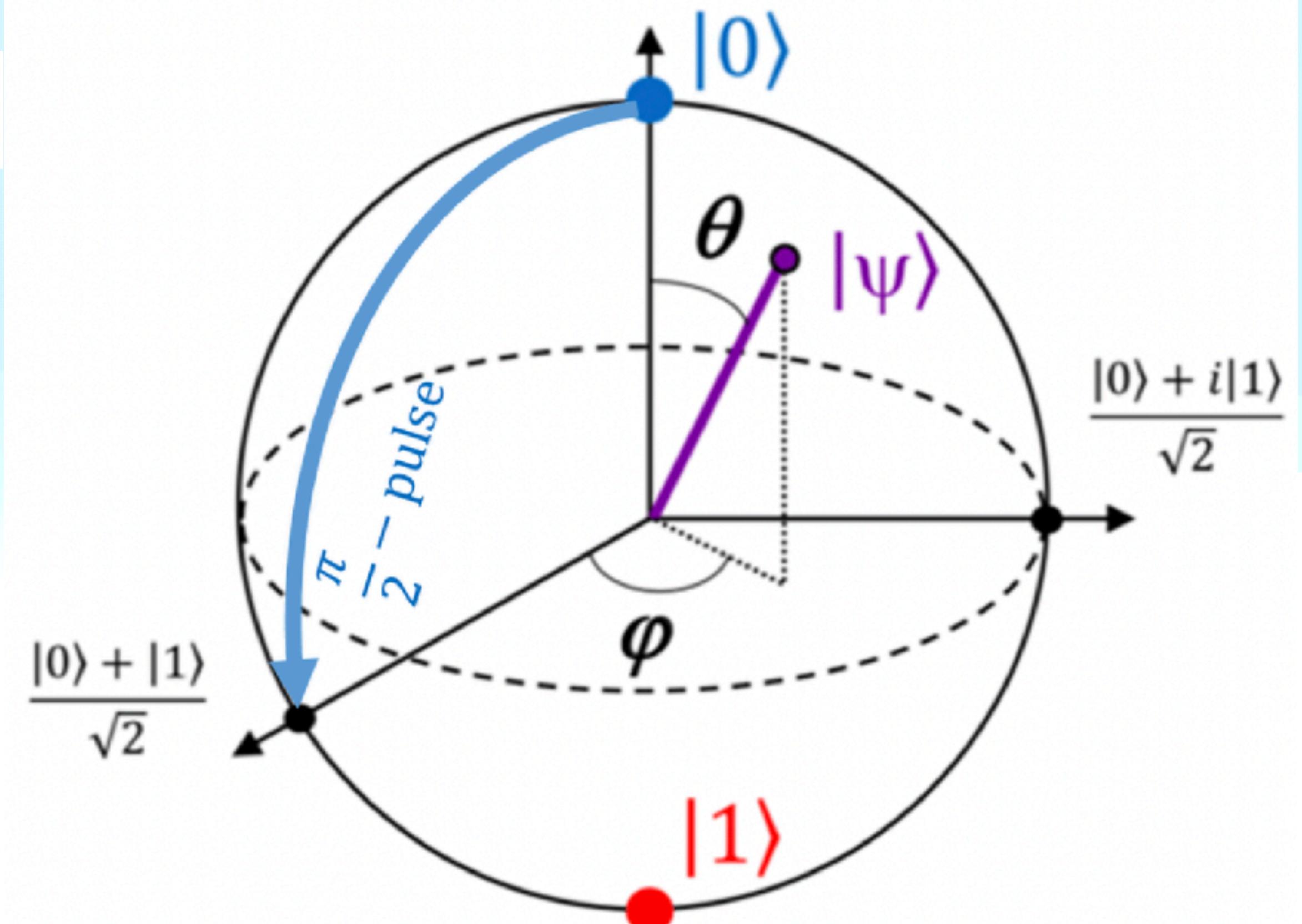
Al medir $|\psi\rangle$ siempre se obtiene $|0\rangle$ o $|1\rangle$
(colapso de la función de onda)

Otras bases posibles para representar el estado de
Superposición de un qubit son:

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \quad |R\rangle = \frac{|0\rangle + i|1\rangle}{\sqrt{2}} \quad |L\rangle = \frac{|0\rangle - i|1\rangle}{\sqrt{2}}$$

$$|+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad |-\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

Esfera de Bloch



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

2.2 Computación Cuántica. Superposición con 2 Qubits

La medición de 2 qubits tiene 2^2 resultados posibles y se representa como la superposición de esos 4 estados base

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$|11\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$$|0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 0 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 \cdot 0 \\ 1 \cdot 1 \\ 0 \cdot 0 \\ 0 \cdot 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1.$$

$$|a\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle = \begin{bmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{bmatrix}$$

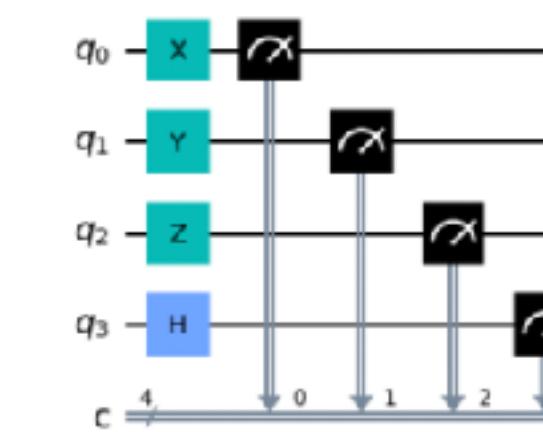
En general un sistema de n qubits se representa como la superposición de 2^n estados base y una medicación colapsa su función de onda a uno de esos estados base

2.3 Computación Cuántica vs Clásica

Classical vs Quantum Computing Terms

Source: Caltech Entrepreneurs Forum, Feb 23, 2019

	Classical	Quantum
Basic Unit	Binary Bit (1 or 0)	Qbit (vector)
Computing	Logical Operation	Unitary Operation
Description	Truth Table (True/False)	Unitary Matrix
Direction	Most Gates Run Forward	Gates are Reversible
Copying	Easy	Impossible
Noise	Minimal w/Error Correction	Quantum Error Correction (Very Difficult)
Storage	n-bit storage holds 1 value. from 0 to $2^{**n} - 1$	n-qbits storage holds 2^{**n} values
Computation	n-bit processor = 1 operation	n-qbit processor = 2^{**n} operations



En computación clásica N bits representan un estado de una computadora clásica (un numero entre 0 y 2^N-1)
En computación cuántica N qubits representan 2^N estados en un espacio vectorial de dimensión 2^N en C

2.3 Computación Cuántica vs Clásica

En computación clásica N bits representan un estado de una computadora clásica (un número entre 0 y 2^N-1)

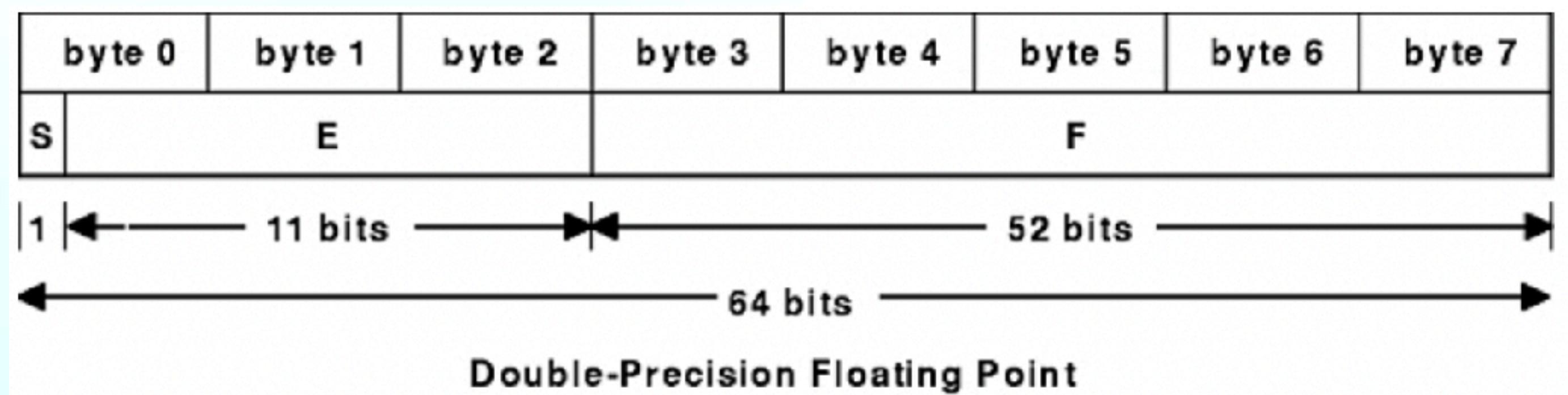
En computación cuántica N qubits representan 2^N estados en un espacio vectorial de dimensión 2^N en los complejos

Para N = 3 qubits

$$|\psi\rangle = \alpha_0|000\rangle + \alpha_1|001\rangle + \alpha_2|010\rangle + \alpha_3|011\rangle + \dots + \alpha_7|111\rangle$$

Para N qubits $|\psi\rangle = \alpha_0|00000\dots000\rangle + \alpha_1|00000..001\rangle + \alpha_2|00000..010\rangle + \dots + \alpha_{2^N-1}|11111..111\rangle$

Para simular una computadora cuántica de N qubits en una clásica requerimos al menos una memoria de $8*2*2^N$ bytes



Por ejemplo para N = 40 se requieren
17.6 TB

Este número tan alto es una motivación en sí para desarrollar computadoras cuánticas para simular procesos cuánticos

2.4 Computación Cuántica. Implementación de los Qubits

Physical support	Name	Information support	$ 0\rangle$	$ 1\rangle$
Photon	Polarization encoding	Polarization of light	Horizontal	Vertical
	Number of photons	Fock state	Vacuum	Single photon state
	Time-bin encoding	Time of arrival	Early	Late
Coherent state of light	Squeezed light	Quadrature	Amplitude-squeezed state	Phase-squeezed state
Electrons	Electronic spin	Spin	Up	Down
	Electron number	Charge	No electron	One electron
Nucleus	Nuclear spin addressed through NMR	Spin	Up	Down
Optical lattices	Atomic spin	Spin	Up	Down
Josephson junction	Superconducting charge qubit	Charge	Uncharged superconducting island ($Q=0$)	Charged superconducting island ($Q=2e$, one extra Cooper pair)
	Superconducting flux qubit	Current	Clockwise current	Counterclockwise current
	Superconducting phase qubit	Energy	Ground state	First excited state
Singly charged quantum dot pair	Electron localization	Charge	Electron on left dot	Electron on right dot
Quantum dot	Dot spin	Spin	Down	Up
Gapped topological system	Non-abelian anyons	Braiding of Excitations	Depends on specific topological system	Depends on specific topological system
Vibrational qubit ^[15]	Vibrational states	Phonon/vibron	$ 01\rangle$ superposition	$ 10\rangle$ superposition
van der Waals heterostructure ^[16]	Electron localization	Charge	Electron on bottom sheet	Electron on top sheet

2.5 Computación Cuántica. Ejemplos de Tecnologías

D-Wave tiene un sistema de 5640 qubits usando su Pegasus chip

Quantum Annealing

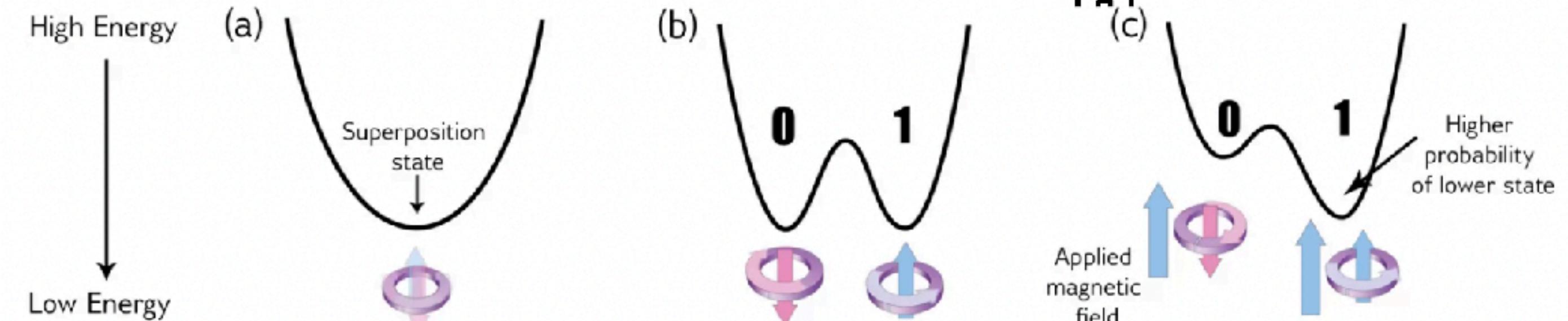


Quantum Hamiltonian is an operator on Hilbert space:

$$\mathcal{H}(t) = \mathcal{E}(t) \left[\sum_i a_i \sigma_i^z + \sum_{i < j} b_{ij} \sigma_i^z \sigma_j^z \right] + \Delta(t) \sum_i \sigma_i^x$$

Corresponding classical optimization problem:

$$\text{Obj}(a_i, b_{ij}; q_i) = \sum_i a_i q_i + \sum_{i < j} b_{ij} q_i q_j$$



Source: [D-Wave](#)

2.5 Computación Cuántica. Ejemplos de Tecnologías

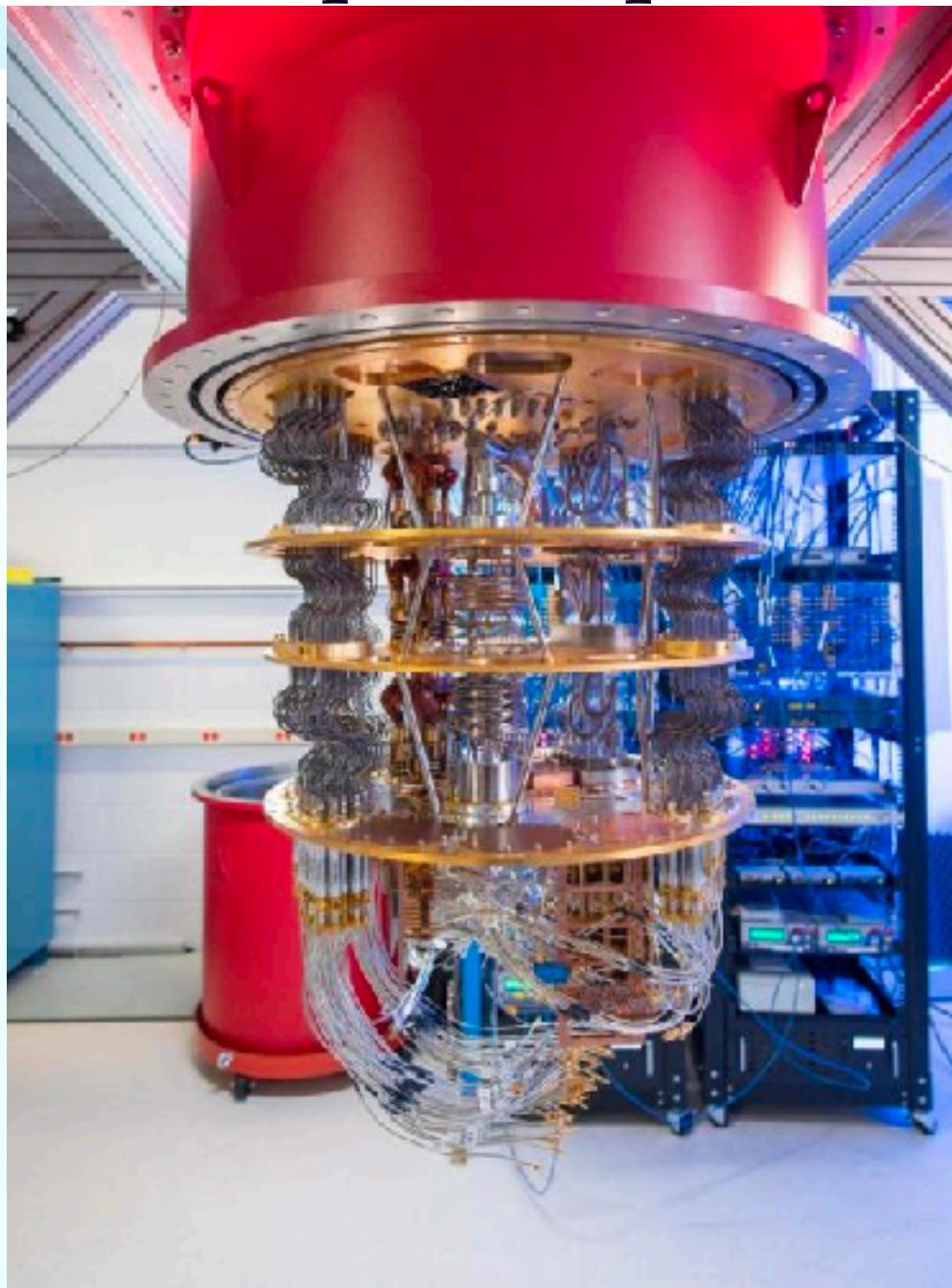
Se logra la “Supremacía Cuántica” cuando un ordenador cuántico es más rápido en la práctica que un ordenador clásico

[nature](#) > [articles](#) > [article](#)

Article | [Published: 23 October 2019](#)

Quantum supremacy using a programmable superconducting processor

Google anunció en Oct/2019 su procesador Sycamore de 53 qubits que toma 200 seg Para resolver un problema que tardaría 10,000 años en una supercomputadora.



Quantum computational advantage using photons

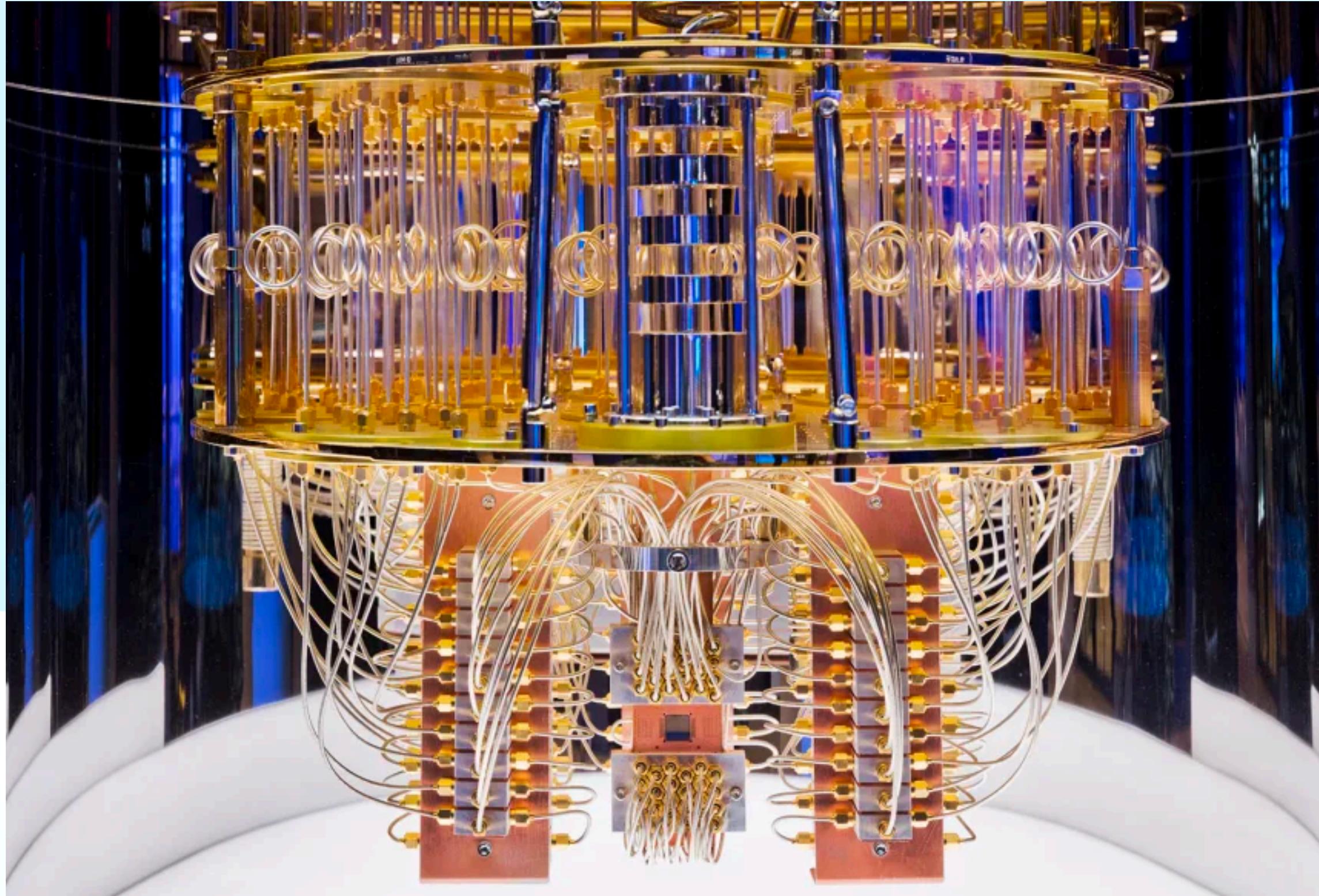
HAN-SEN ZHONG , HUI WANG , YU-HAO DENG , MING-CHENG CHEN , LI-CHAO PENG , YI-HAN LUO , JIAN QIN , DIAN WU , XING DING  [...] AND JIAN-WEI PAN  +14 authors [Authors Info & Affiliations](#)

SCIENCE • 3 Dec 2020 • Vol 370, Issue 6523 • pp. 1460-1463 • DOI: 10.1126/science.abe8770

China en Dic/2020 publicó en Science un artículo detallando la solución mediante un computador cuántico en cerca de tres minutos un problema en el que los superordenadores clásicos tardarían 600 millones de años.

2.5 Computación Cuántica. Ejemplos de Tecnologías

IBM logra 433 qubits con su procesador Osprey en noviembre de 2022



IBM planea sus procesadores Condor de 1121 qubits para 2023, los Flamingo de 1386 qubits para 2024 y el procesador Kookaburra de 4.000 qubits para 2025

QC company examples	<ul style="list-style-type: none">• Honeywell: Trapped ion• IonQ: Trapped ion• PsiQuantum: Photonics• Xanadu: Photonics• Cold Quanta: Natural atom	<ul style="list-style-type: none">• D-Wave: Superconducting• Google: Superconducting• IBM: Superconducting• Intel: Superconducting• Rigetti: Superconducting
---------------------	--	--

Source: Egil Juliussen, January 2022

3. Compuertas Cuánticas

Las compuertas cuánticas se representan como matrices.

Una compuerta que opera sobre n qubits queda representada por una matriz unitaria de $2^n \times 2^n$. Las operaciones s U son reversibles a diferencia de la computación clásica

Gate	Equation	Matrix	Transform	Notation
Identity (I)	$I = 0\rangle\langle 0 + 1\rangle\langle 1 $	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$I 0\rangle = 0\rangle$ $I 1\rangle = 1\rangle$	
Pauli-X (X or NOT)	$X = 0\rangle\langle 1 + 1\rangle\langle 0 $	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$X 0\rangle = 1\rangle$ $X 1\rangle = 0\rangle$	
Hadamard (H)	$H = \frac{ 0\rangle+ 1\rangle}{\sqrt{2}}\langle 0 + \frac{ 0\rangle- 1\rangle}{\sqrt{2}}\langle 1 $	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	$H 0\rangle = \frac{1}{\sqrt{2}}(0\rangle + 1\rangle)$ $H 1\rangle = \frac{1}{\sqrt{2}}(0\rangle - 1\rangle)$	
Controlled-NOT (CNOT)	$CNOT = 0\rangle\langle 0 \otimes I + 1\rangle\langle 1 \otimes X$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$	$CNOT 00\rangle = 00\rangle$ $CNOT 01\rangle = 01\rangle$ $CNOT 10\rangle = 11\rangle$ $CNOT 11\rangle = 10\rangle$	
Toffoli (T or CCNOT)	$T = 0\rangle\langle 0 \otimes I \otimes I + 1\rangle\langle 1 \otimes CNOT$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$	$T 000\rangle = 000\rangle, T 001\rangle = 001\rangle$ $T 010\rangle = 010\rangle, T 011\rangle = 011\rangle$ $T 100\rangle = 100\rangle, T 101\rangle = 101\rangle$ $T 110\rangle = 111\rangle, T 111\rangle = 110\rangle$	

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

$$X|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

$$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$Y = -i|0\rangle\langle 1| + i|1\rangle\langle 0|$$

$$|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$|1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$Z = |0\rangle\langle 0| - |1\rangle\langle 1|$$

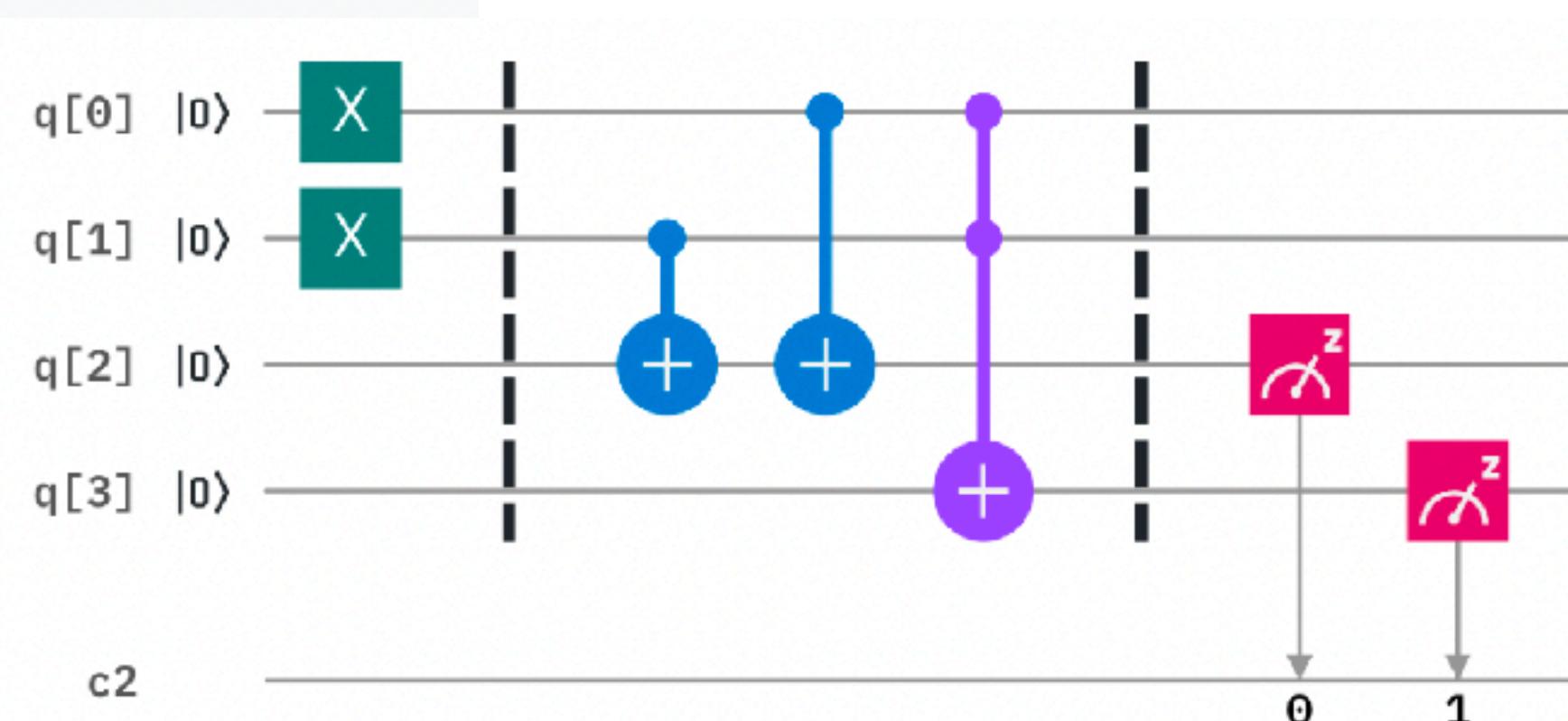
4. Introducción a Python y a la Programación Cuántica con Qiskit

Qiskit es un Kit de Desarrollo de Software (SDK) creado por IBM de código abierto para programación cuántica usando Python.

Sigue el modelo de circuito para la computación cuántica universal y se puede utilizar para cualquier hardware cuántico que use este modelo.

Ejemplos de un programa y un circuito

```
from qiskit import QuantumCircuit  
  
qc = QuantumCircuit(2, 2)  
  
qc.h(0)  
qc.cx(0, 1)  
qc.measure([0,1], [0,1])
```



Learn Quantum Computation using Qiskit

<https://qiskit.org/textbook/preface.html>

Vamos a hacer más ejemplos usando Google Colab

<https://github.com/Qiskit/qiskit-tutorials>

5. Parte Práctica del Primer Taller

Para esta parte práctica las instrucciones son las siguientes:

- Clonar el repositorio creado para este Taller con el comando. Si es necesario primero instalar con el comando *sudo apt install git* (linux)
- ***git clone <https://github.com/lvillasen/Introduccion-a-la-Computacion-Cuantica.git>***
- Copiar el cuaderno de jupyter (con terminación ipynb) a Google Drive
- Entrar a la página de Google Drive con un explorador y abrir el archivo en Google Colab

Para saber más sobre Programación Cuántica

CERN lectures on quantum computing

Noviembre 2020

- Lecture 1/7, Friday 6 November: [Introduction](#)
- Lecture 2/7, Friday 13 November: [One and two-qubit systems \(Part 1\)](#)
- Lecture 3/7, Friday 20 November: [One and two-qubit systems \(Part 2\)](#)
- Lecture 4/7, Friday 27 November: [Multiqubit systems](#)
- Lecture 5/7, Friday 4 December: [Quantum algorithms for combinatorial optimization](#)
- Lecture 6/7, Friday 11 December: [Quantum variational algorithms and quantum machine learning](#)
- Lecture 7/7, Friday 18 December: [The future of quantum computing](#)

Quantum Computing Workshop 2020

https://github.com/mnp-club/Quantum_Computing_Workshop_2020

Primera Escuela de Computación Cuántica Octubre 2022

<https://www.youtube.com/channel/UCCUrwQCi5EO-L6xWGF1Jh0Q>

Quantum-Computing-Collection-Of-Resources

<https://github.com/aryashah2k/Quantum-Computing-Collection-Of-Resources>



Welcome to Quirk

A drag-and-drop quantum circuit simulator.

<https://algassert.com/quirk>

Real quantum computers.
Right at your fingertips.

<https://quantum-computing.ibm.com/>

Open-Source Quantum Development

<https://qiskit.org/>

Learn Quantum Computation using Qiskit

<https://qiskit.org/textbook/preface.html>

www.youtube.com/watch?v=0Av89fZenSY&t=0s

[Products](#) / [Quantum Technologies](#) / [Amazon Braket](#)

Amazon Braket Getting Started

<https://github.com/aws/amazon-braket-examples>

Google Colaboratory



Understanding
Quantum
Information & Computation

#qiskit #quantumcomputing #learnquantum

Quantum Computing Book Recommendations

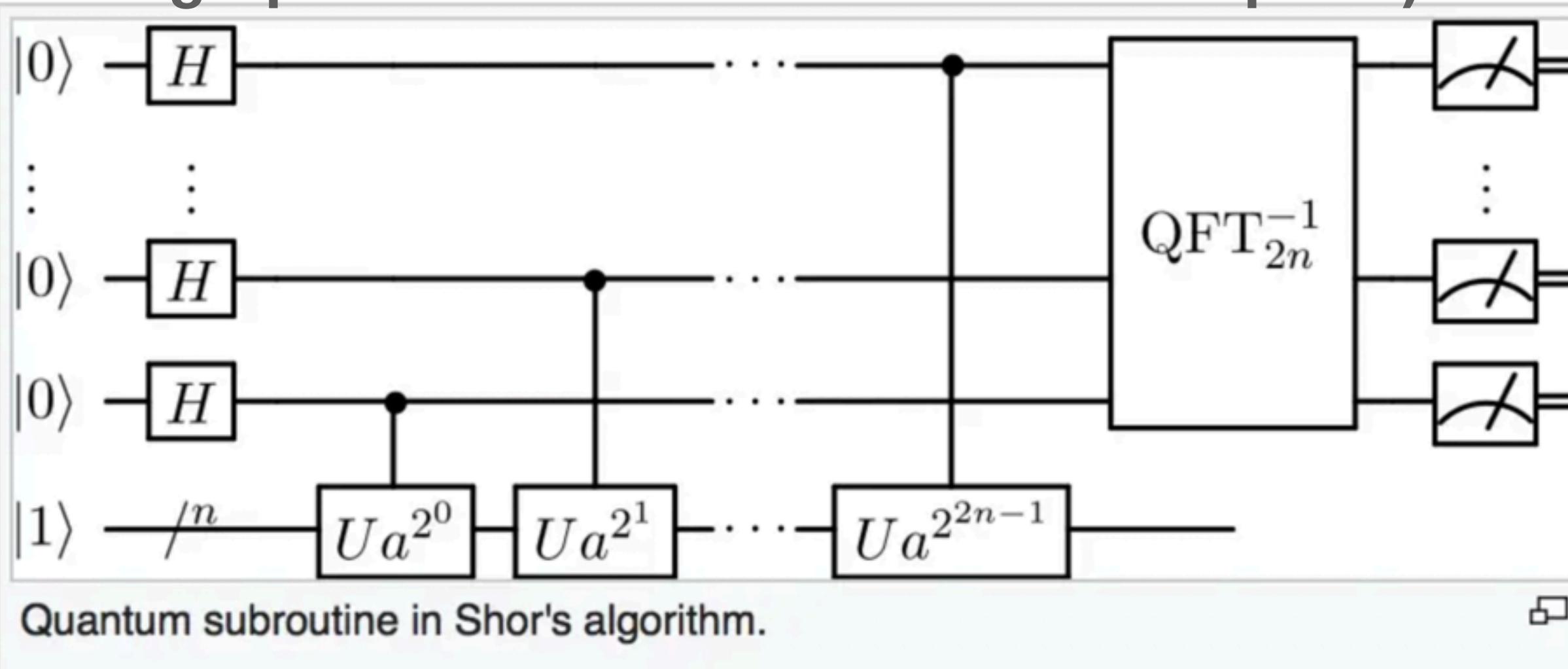


Subscribe

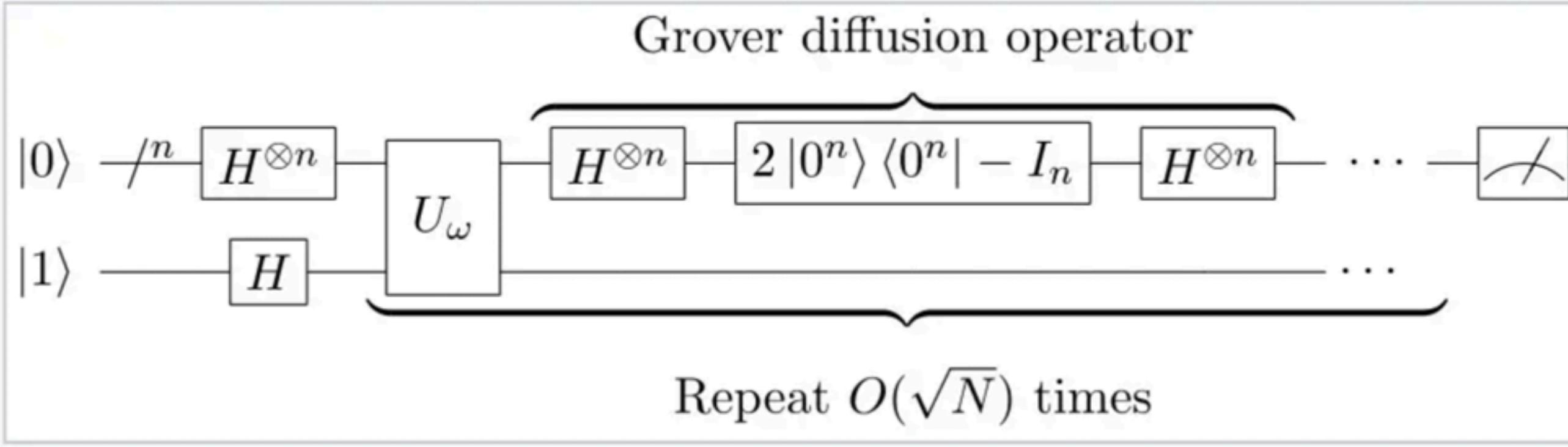
www.youtube.com/watch?v=xpSevVullcQ

Segundo Taller. Algoritmos Cuánticos

Algoritmo de Factorización de Shor (1994. En 2001
un grupo de IBM factorizó 15 usando 7 qubits)



Algoritmo de Búsqueda de Grover ($O(N^{1/2})$, 1996)



En 2019 se demostró que un ordenador cuántico podría hacer el cálculo de RSA-2048 con solo 20 millones de cúbits en ocho horas

arXiv > quant-ph > arXiv:1905.09749

Quantum Physics

[Submitted on 23 May 2019 (v1), last revised 13 Apr 2021 (this version, v3)]

How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits

Craig Gidney, Martin Ekerå

Para saber más sobre Algoritmos Cuánticos

quantumalgorithmzoo.org

Quantum Algorithm Zoo

This is a comprehensive catalog of quantum algorithms. If you notice any errors or omissions, please email me at stephen.jordan@microsoft.com. (Alternatively, you may submit a pull request to the [repository](#) on github.) Your help is appreciated and will be [acknowledged](#).



Quantum Physics

[Submitted on 24 Aug 2020]

Fundamentals In Quantum Algorithms: A Tutorial Series Using Qiskit Continued

Daniel Koch, Saahil Patel, Laura Wessing, Paul M. Alsing

Para saber más sobre Algoritmos Cuánticos

quantumalgorithmzoo.org

Quantum Algorithm Zoo

This is a comprehensive catalog of quantum algorithms. If you notice any errors or omissions, please email me at stephen.jordan@microsoft.com. (Alternatively, you may submit a pull request to the [repository](#) on github.) Your help is appreciated and will be [acknowledged](#).

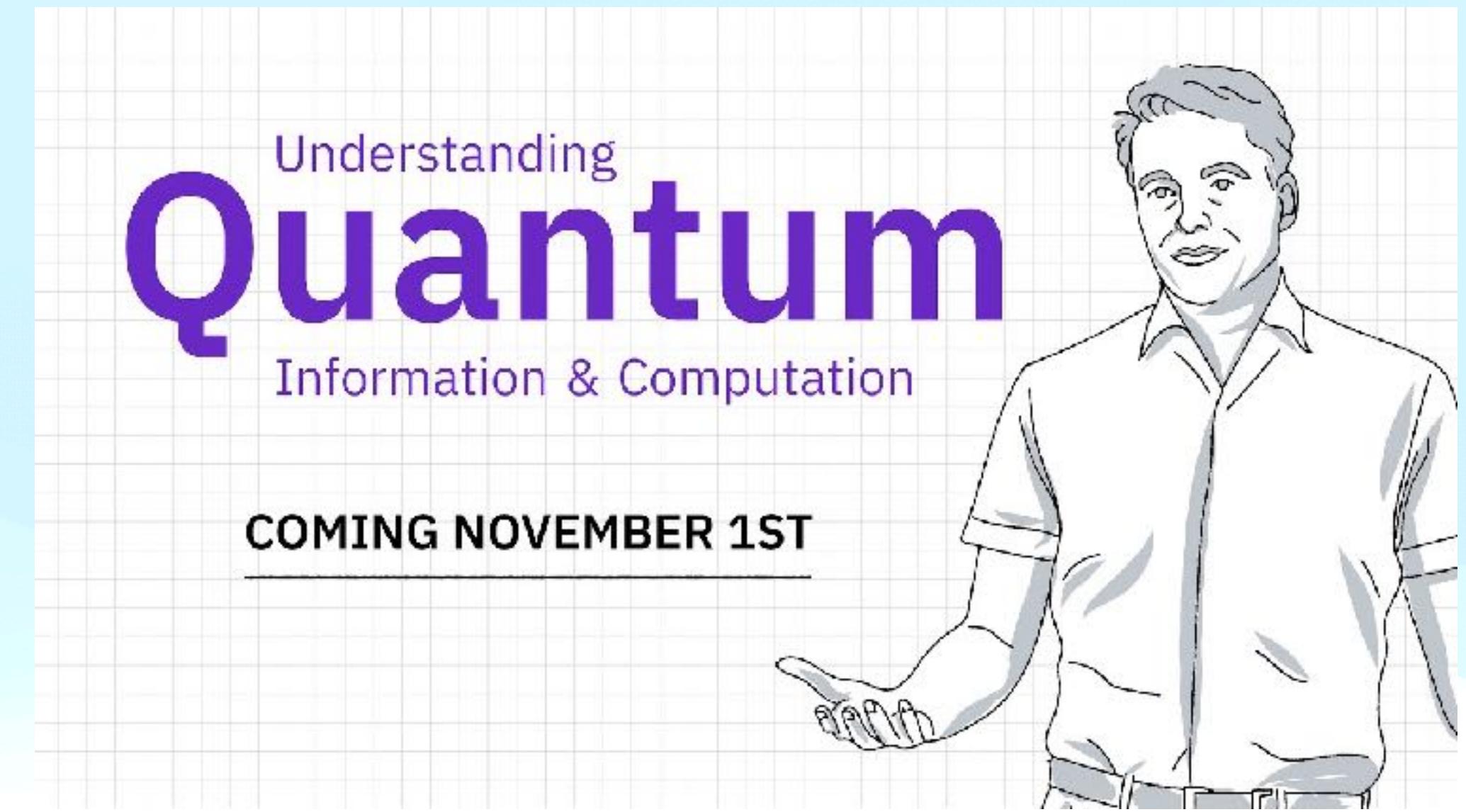
arXiv > quant-ph > arXiv:2008.10647

Quantum Physics

[Submitted on 24 Aug 2020]

Fundamentals In Quantum Algorithms: A Tutorial Series Using Qiskit Continued

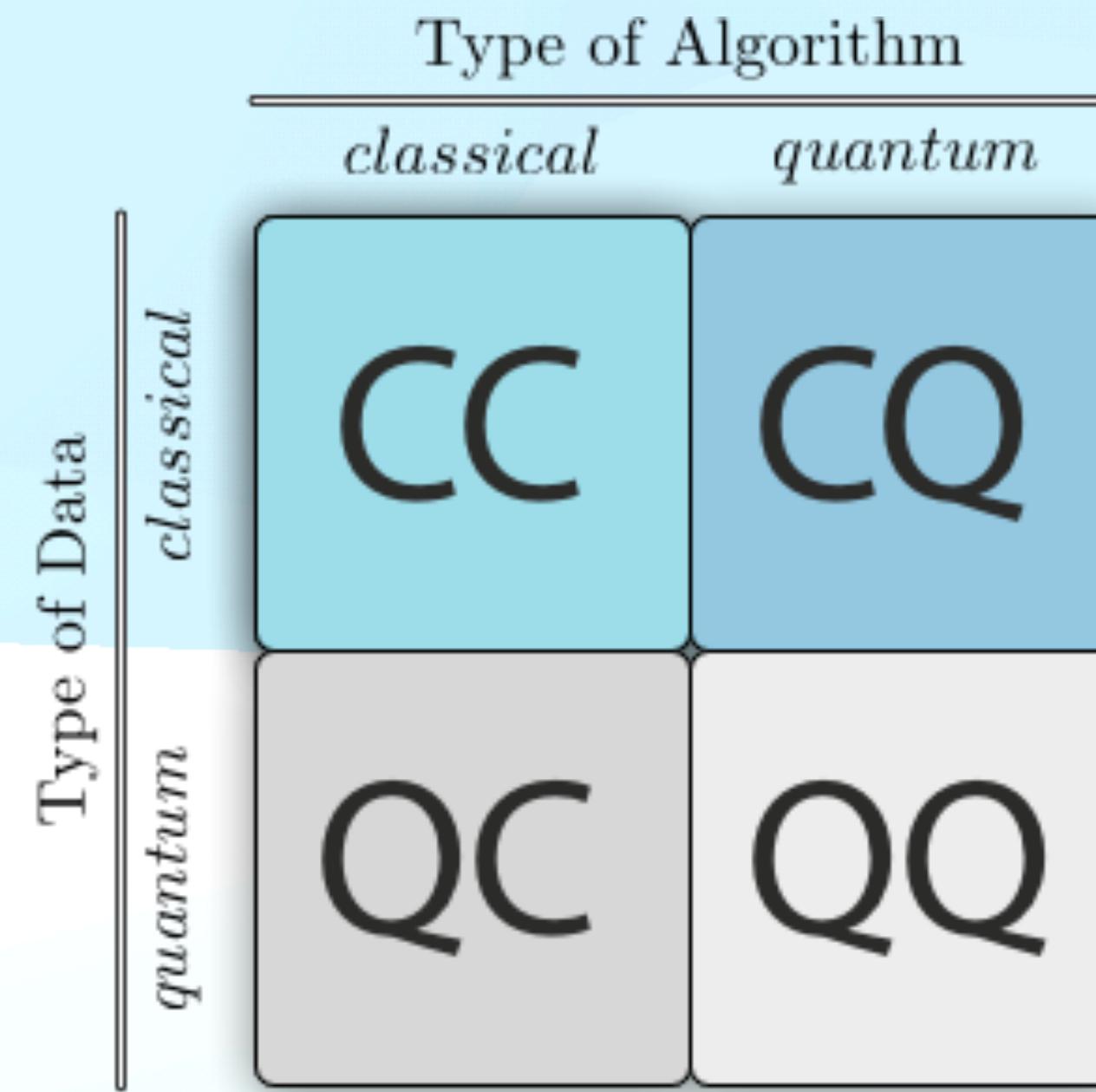
Daniel Koch, Saahil Patel, Laura Wessing, Paul M. Alsing



www.youtube.com/watch?v=0Av89fZenSY

Tercer Taller. Machine Learning con Computación Cuántica

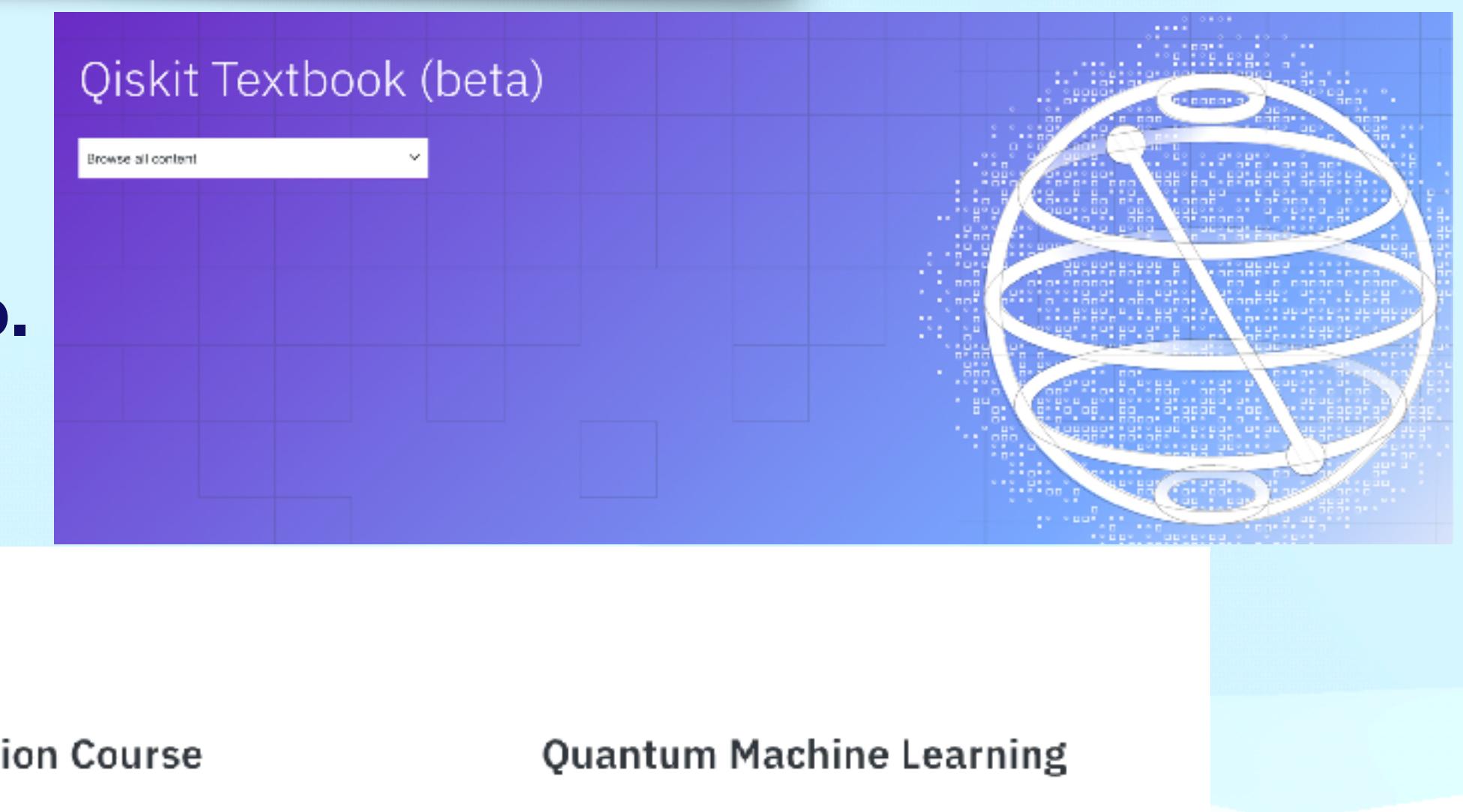
El área de desarrollo de algoritmos cuánticos para machine learning está una etapa inicial de rápido desarrollo.



La esperanza es que el aprendizaje cuántico revolucione el campo de la inteligencia artificial en el futuro próximo.

Courses

Basics of quantum information	Introduction Course	Quantum Machine Learning
Single systems	Why Quantum Computing?	Introduction
Multiple systems	The Atoms of Computation	Parameterized quantum circuits
Circuits, protocols, and games	What is Quantum?	Data encoding
	Describing Quantum Computers	Training parameterized quantum circuits
	Entangled States	Supervised learning
	Visualizing Entanglement	Variational classification
	Grover's search algorithm	Quantum feature maps and kernels
	Project	Unsupervised learning
		Quantum generative adversarial networks
		Project



Introducción a la Computación Cuántica

Segundo Taller

Luis Villaseñor
Profesor Visitante
CIIEC-BUAP
Profesor de Asignatura
ENES Morelia UNAM

02/Febrero/2023

Contenido del Segundo Taller

6. Desigualdad de Bell

7. Repaso del Primer Taller

8. Uso de una Computadora Cuántica Real de IBM Quantum Experience

9. Criptografía Clásica. Algoritmo RSA

9.1 Algoritmo Extendido de Euclides

9.2 Exponenciación Modular

9.2 Un Ejemplo de Encriptación RSA

9.3 Pequeño Teorema de Fermat

9.4 Sustento Matemático de la Encriptación RSA

10. Algoritmo de Shor (Peter Shor, 1994)

10.1 Cálculo del Periodo usando Computación Clásica

10.2 Transformada Discreta de Fourier

10.3 Cálculo del Periodo usando Computación Cuántica

10.3.1 Quantum Fourier Transform

10.3.2 Factorización del Número 21

11. Código Superdenso

12. Criptografía Cuántica. Protocolo de Distribución de Clave BB8

Parte Práctica con Jupyter Notebook en Google Colab

En el siguiente link podrán descargar el material del taller

<https://github.com/lvillasen/Introduccion-a-la-Computacion-Cuantica>

6. Desigualdad de Bell

Paradoja EPR en 1935



A. Einstein

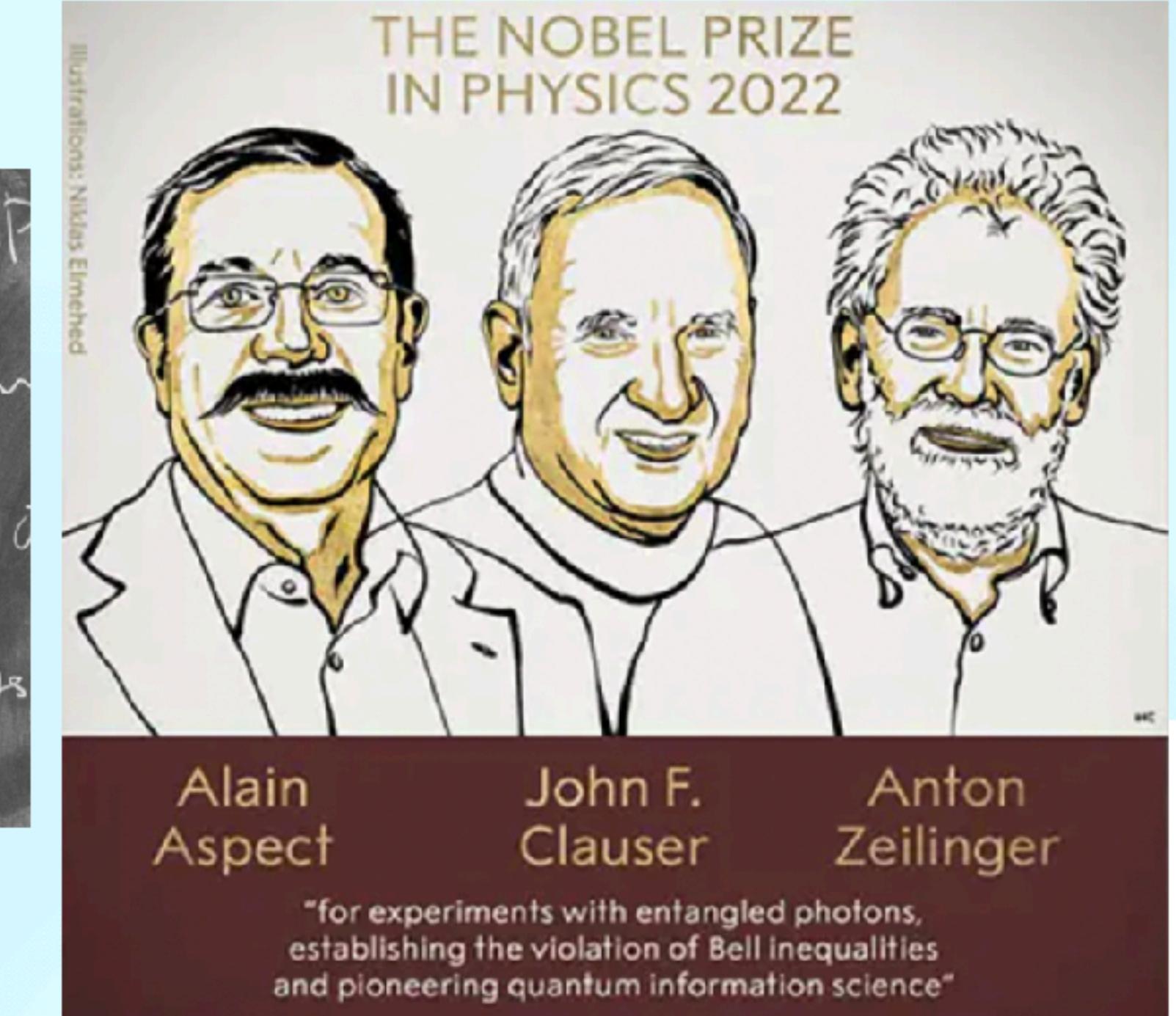
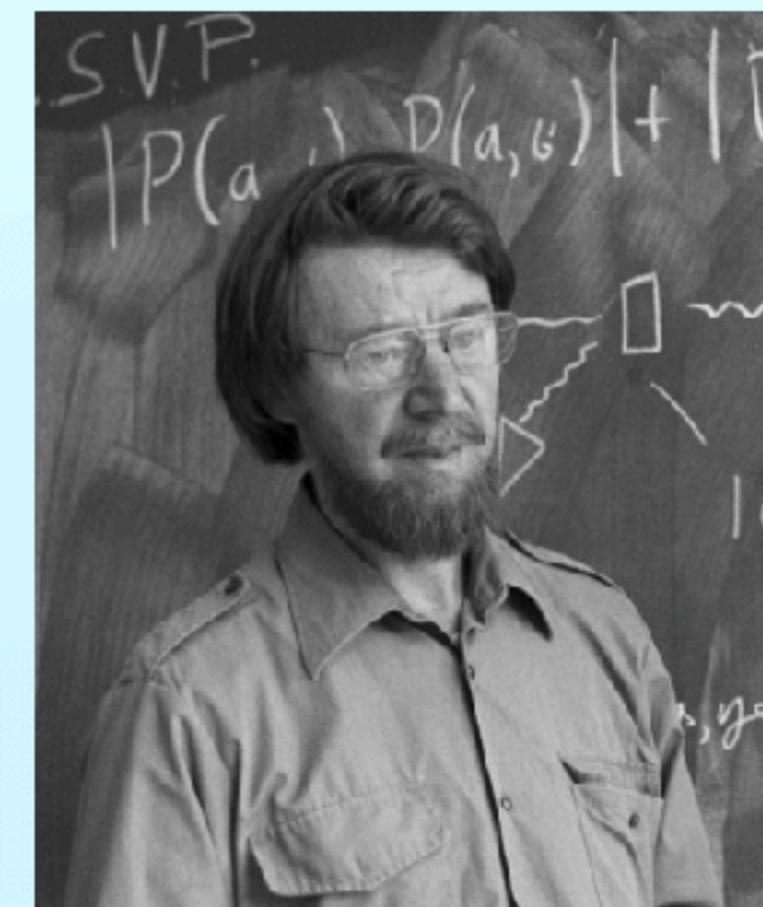


B. Podolsky



N. Rosen

Desigualdad de Bell en 1964



Brian Green



Your Daily Equation #21: Bell's Theorem and the Non-locality of the Universe

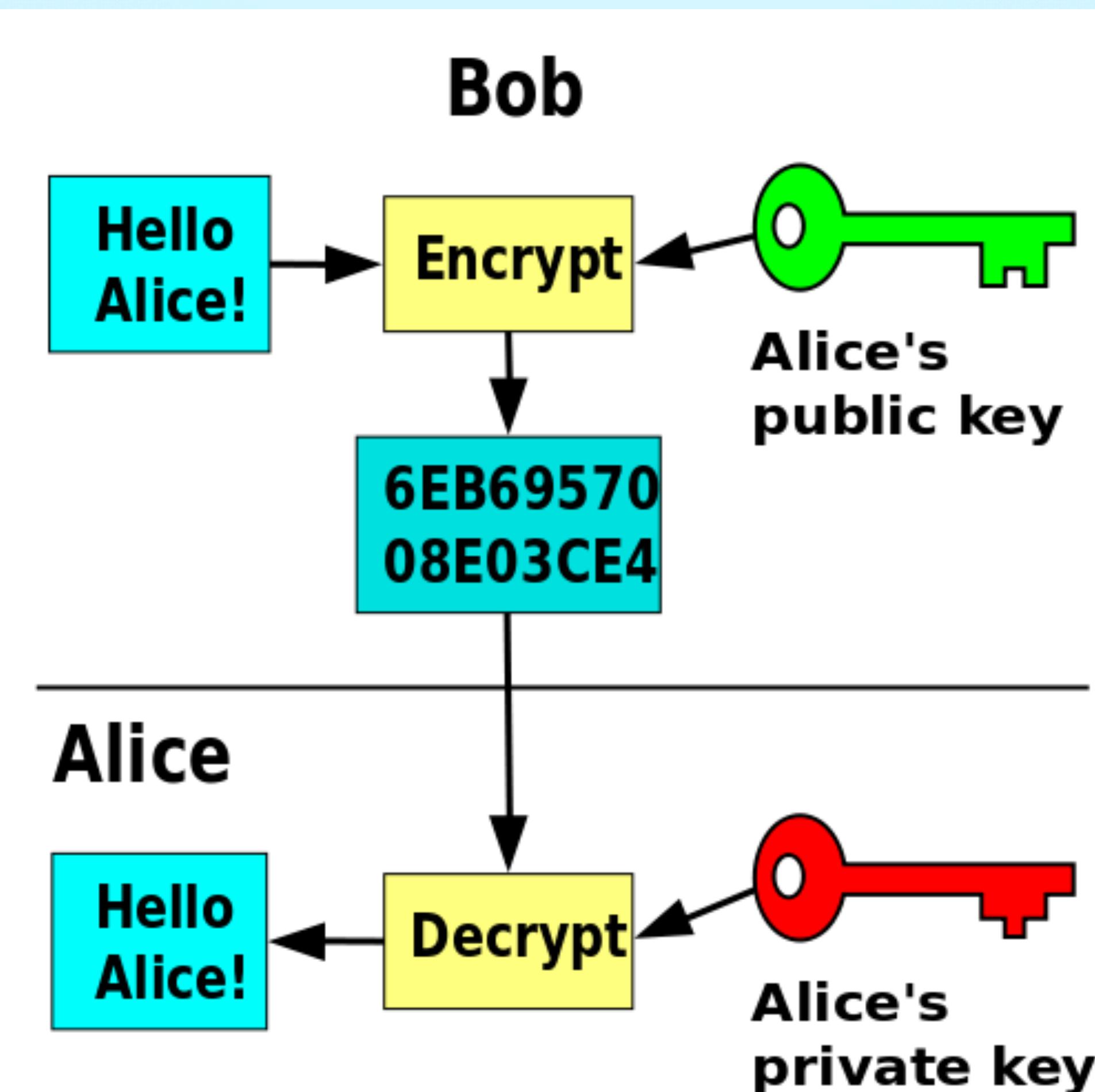
A popular exposition of Bell's theorem can be found in N.D.Mermin, “Bringing home the atomic world: Quantum mysteries for anybody”, Am. J. Phys. 49, 940-3 (1981). An expanded version of this paper can be found as Ch.12 in N.D.Mermin, *Boojums all the way through* (Cambridge U.P., Cambridge, 1990). See also N.D.Mermin, “Is the moon there when nobody looks? Reality and the quantum theory”, Phys. Today 38 (4), 38-47 (1985).

7. Repaso del Primer Taller en Parte Práctica

**8. Uso de una Computadora Cuántica Real de
IBM Quantum Experience en Parte Práctica**

9. Criptografía Clásica. Cifrado RSA

RSA (Ron Rivest, Adi Shamir y Leonard Adleman, del MIT, 1977);
Es un algoritmo de cifrado asimétrico, es decir que usa 2 llaves diferentes, la pública y la privada.



9. Criptografía Clásica. Cifrado RSA

Generación de las llaves pública y privada

1. Generar 2 primos p y q
2. Definir el *semiprimo*

$$N = p * q$$

3. Definir

$$\phi = (p - 1) * (q - 1)$$

Llamada función indicatriz de Euler o función totiente

4. Generar la llave de encriptación e tal que

$$MCD(e, \phi) = 1$$

donde e está entre 1 y $\phi - 1$

Llave Pública: (e, N)

visible para todo mundo

5. Generar la llave de desencriptación d tal que d es el inverso multiplicativo de e módulo ϕ

$$d * e \equiv 1 \pmod{\phi}$$

Llave Privada: (d, N)

solo la tiene el destinatario del mensaje encriptado.

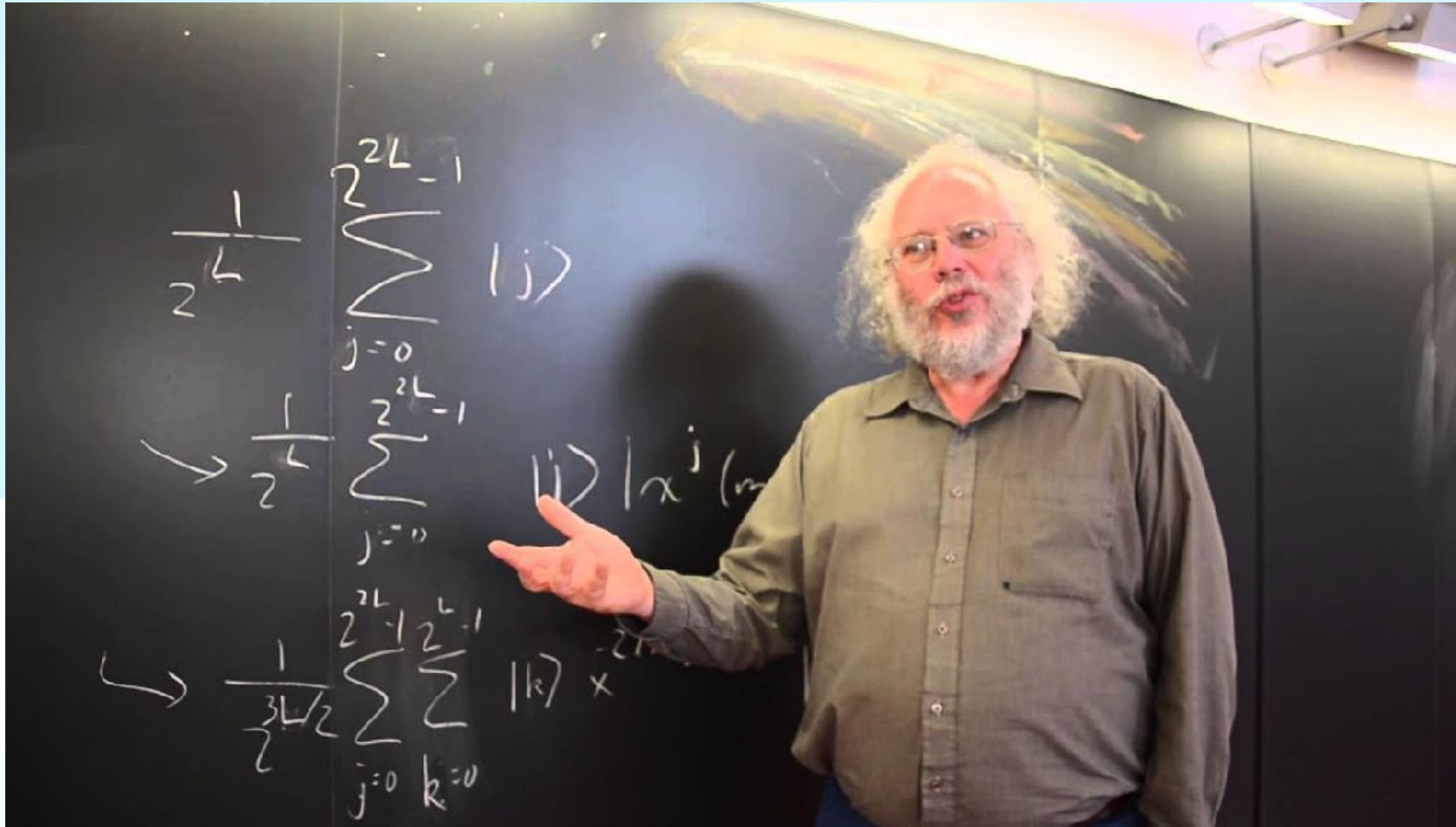
6. Encriptación del mensaje m para producir m'

$$m' = m^e \pmod{N}$$

7. Desencriptación del mensaje m' para obtener m

$$m = m'^d \pmod{N}$$

10. Algoritmos de Shor (Peter Shor, 1994)



Fuente: [youtube.com/watch?v=hOIOY7NyMfs&t=75s](https://www.youtube.com/watch?v=hOIOY7NyMfs&t=75s)

Otra Referencia

<https://medium.com/mit-6-s089-intro-to-quantum-computing/a-general-implementation-of-shors-algorithm-da1595694430>

Shor's Algorithm for Factoring Large Integers*

C. Lavor[†], L.R.U. Manssur[‡], and R. Portugal[‡]

[†]Instituto de Matemática e Estatística

Universidade do Estado do Rio de Janeiro - UERJ

Rua São Francisco Xavier, 524, 6ºandar, bl. D, sala 6018,
Rio de Janeiro, RJ, 20550-900, Brazil

e-mail: carlige@ime.uerj.br

[‡]Coordenação de Ciência da Computação

Laboratório Nacional de Computação Científica - LNCC

Av. Getúlio Vargas 333, Petrópolis, RJ, 25651-070, Brazil

e-mail: {leon, portugal}@lncc.br

February 1, 2008

Abstract

This work is a tutorial on Shor's factoring algorithm by means of a worked out example. Some basic concepts of Quantum Mechanics and quantum circuits are reviewed. It is intended for non-specialists which have basic knowledge on undergraduate Linear Algebra.

1 Introduction

In the last 30 years, the number of transistors per chip roughly doubled every 18 months, amounting to an exponentially growing power of classical computers. Eventually this statement (Moore's law) will be violated, since the transistor size will reach the limiting size of one atom in about 15 years. Even before that, disturbing quantum effects will appear.

10. Algoritmos de Shor (Peter Shor, 1994)

1. Choose $T = 2^t$ such that $N^2 \leq T \leq 2N^2$. Initialise two registers of qubits, first an argument register with t qubits and second a function register with $n = \log_2 N$ qubits. These registers start in the initial state:

$$|\psi_0\rangle = |0\rangle|0\rangle$$

2. Apply a Hadamard gate on each of the qubits in the argument register to yield an equally weighted superposition of all integers from 0 to T :

$$|\psi_1\rangle = \frac{1}{\sqrt{T}} \sum_{a=0}^{T-1} |a\rangle|0\rangle$$

3. Implement the modular exponentiation function $x^a \bmod N$ on the function register, giving the state:

$$|\psi_2\rangle = \frac{1}{\sqrt{T}} \sum_{a=0}^{T-1} |a\rangle|x^a \bmod N\rangle$$

This $|\psi_2\rangle$ is highly entangled and exhibits quantum parallelism, i.e. the function entangled in parallel all the 0 to T input values with the corresponding values of $x^a \bmod N$, even though the function was only executed once.

4. Perform a quantum Fourier transform on the argument register, resulting in the state:

$$|\psi_3\rangle = \frac{1}{T} \sum_{a=0}^{T-1} \sum_{z=0}^{T-1} e^{(2\pi i)(az/T)} |z\rangle|x^a \bmod N\rangle$$

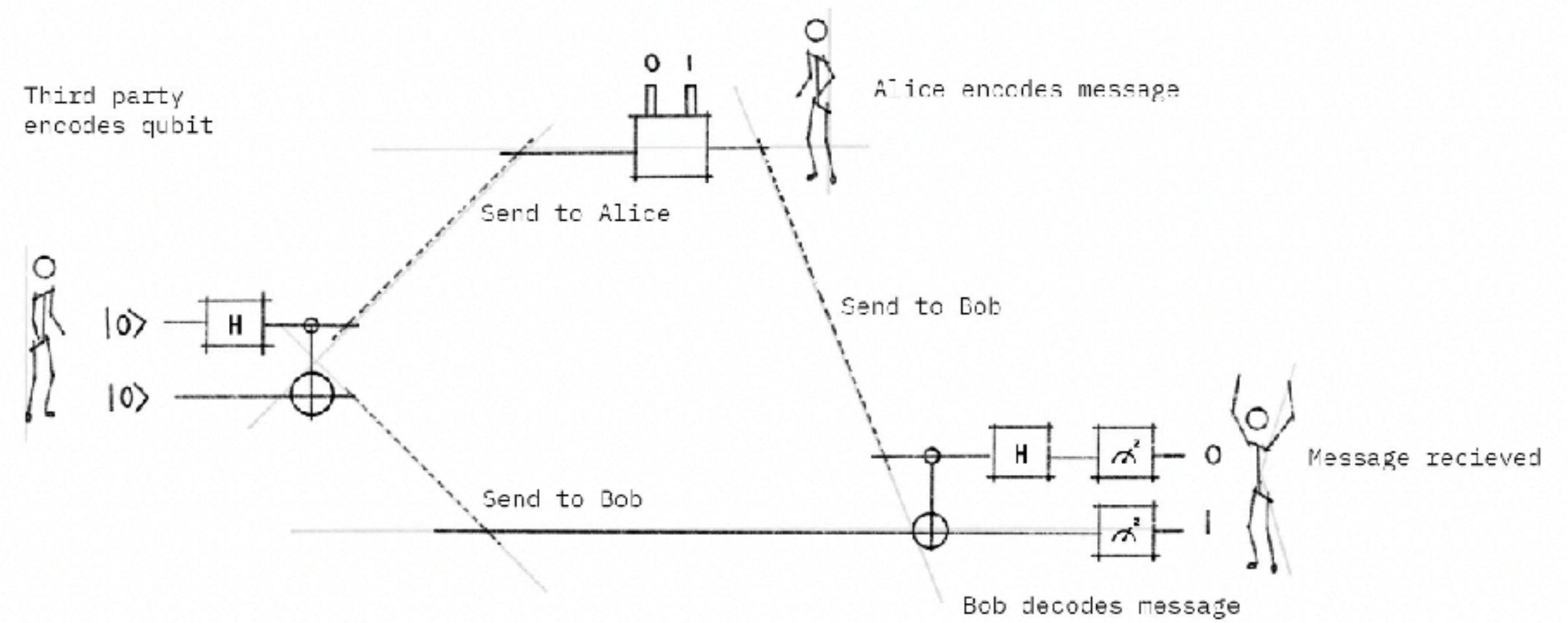
where due to the interference, only the terms $|z\rangle$ with

$$z = qT/r$$

have significant amplitude where q is a random integer ranging from 0 to $r - 1$ and r is the period of $\mathcal{F}(a) = x^a \bmod N$.

5. Measure the argument register to obtain classical result z . With reasonable probability, the continued fraction approximation of T/z will be an integer multiple of the period r . Euclid's algorithm can then be used to find r .

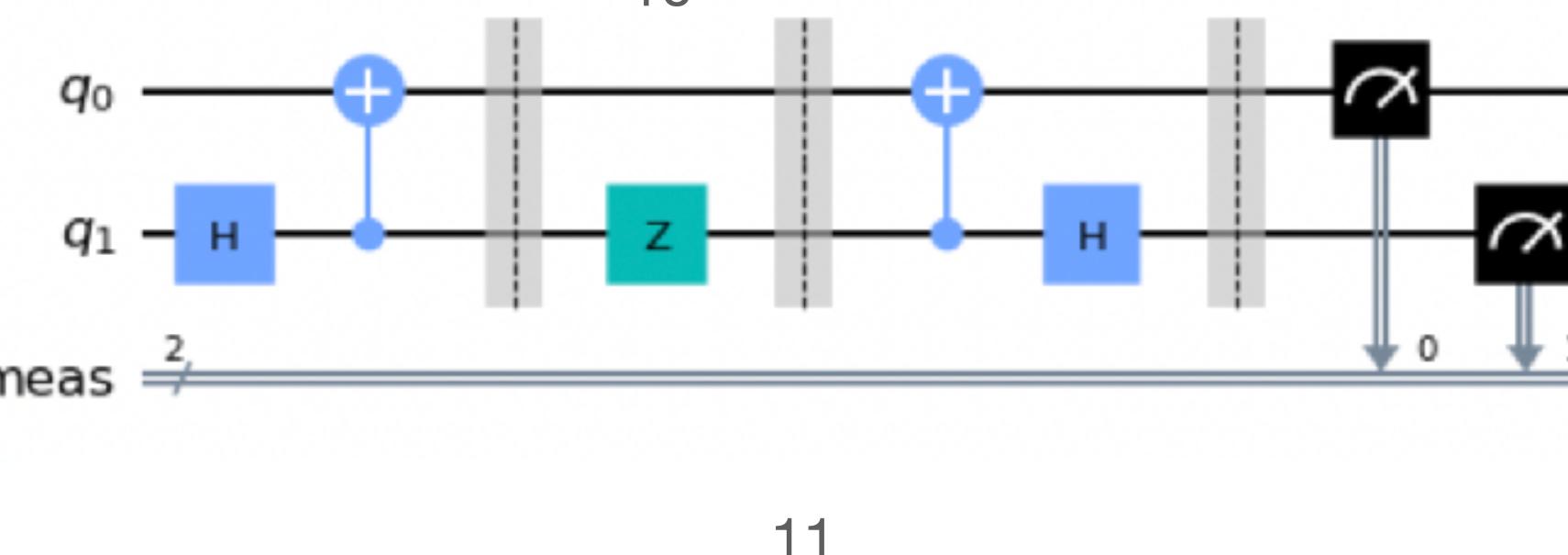
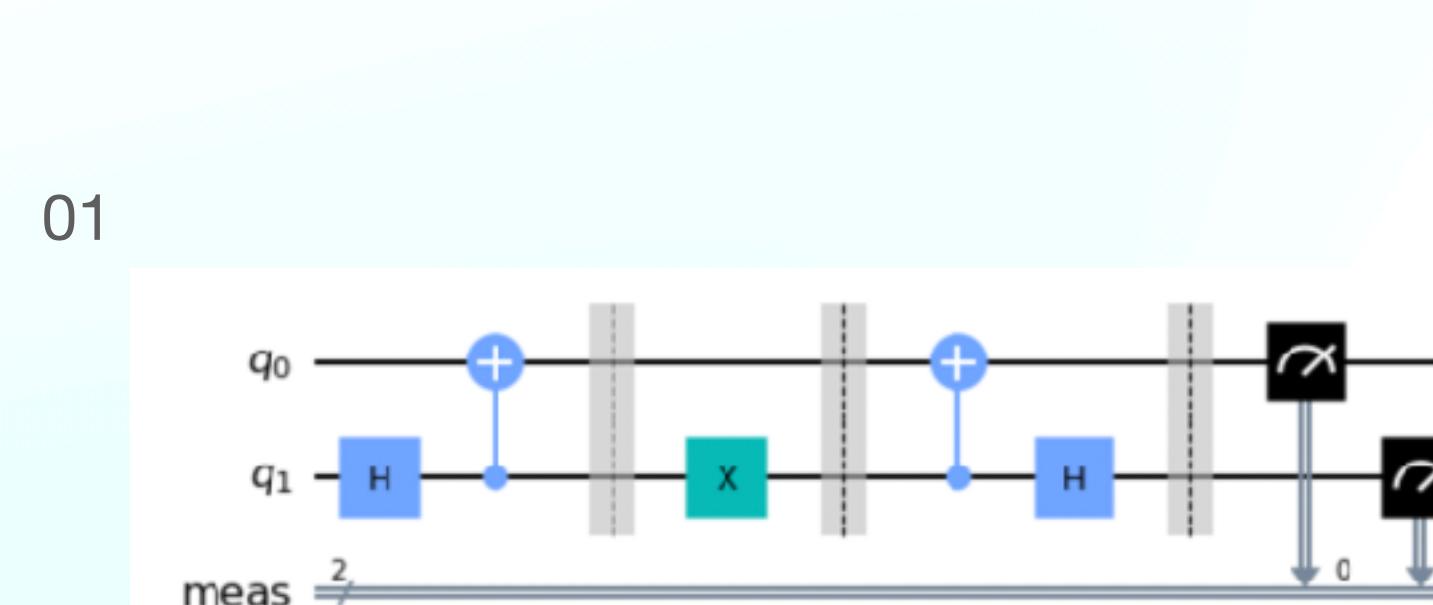
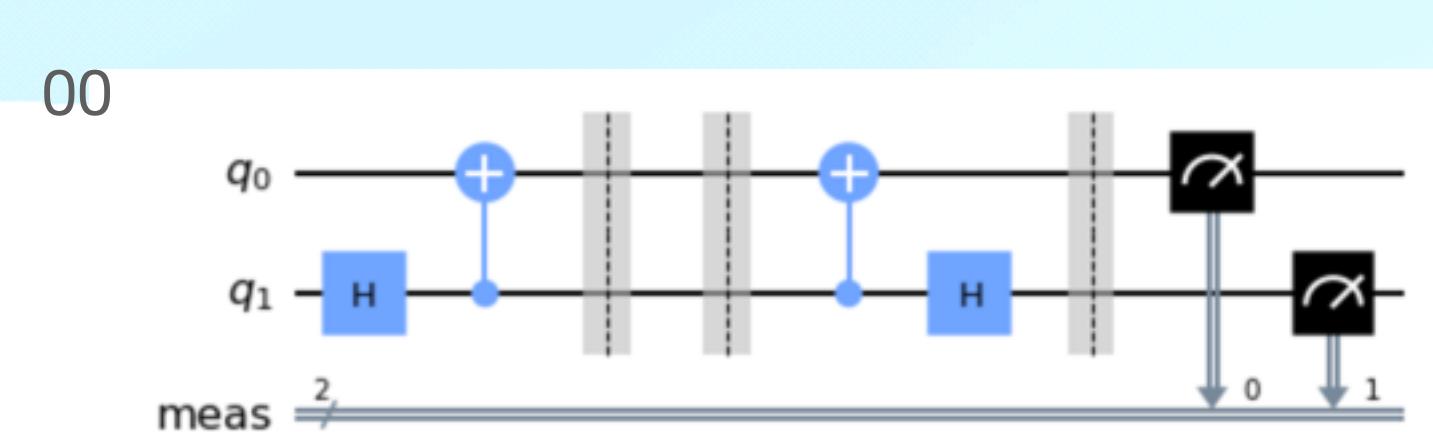
11. Código Superdenso. Charles H. Bennett and Stephen Wiesner, 1970



Fuente: <https://qiskit.org/textbook/ch-algorithms/superdense-coding.html>

Envío de 2 bits de información mediante un qubit

Teleportation	Superdense Coding
Transmit one qubit using two classical bits	Transmit two classical bits using one qubit



Intended Message	Applied Gate	Resulting State ($\cdot \frac{1}{\sqrt{2}}$)
00	I	$ 00\rangle + 11\rangle$
01	X	$ 10\rangle + 01\rangle$
10	Z	$ 00\rangle - 11\rangle$
11	ZX	$- 10\rangle + 01\rangle$

Bob Receives ($\cdot \frac{1}{\sqrt{2}}$)	After CNOT-gate ($\cdot \frac{1}{\sqrt{2}}$)	After H-gate
$ 00\rangle + 11\rangle$	$ 00\rangle + 10\rangle$	$ 00\rangle$
$ 10\rangle + 01\rangle$	$ 11\rangle + 01\rangle$	$ 01\rangle$
$ 00\rangle - 11\rangle$	$ 00\rangle - 10\rangle$	$ 10\rangle$
$- 10\rangle + 01\rangle$	$- 11\rangle + 01\rangle$	$ 11\rangle$

12. Criptografía Cuántica. Protocolo de Distribución de Clave BB84

Protocolo publicado en 1984 por Charles Bennett y Gilles Brassard
Da origen a la criptografía cuántica

