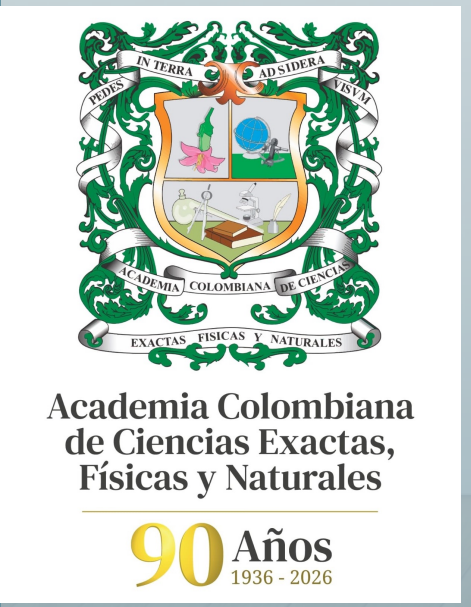
DE LA COMPUTACIÓN CLÁSICA A LA COMPUTACIÓN QUANTICA

ROBERTO MARTÍNEZ

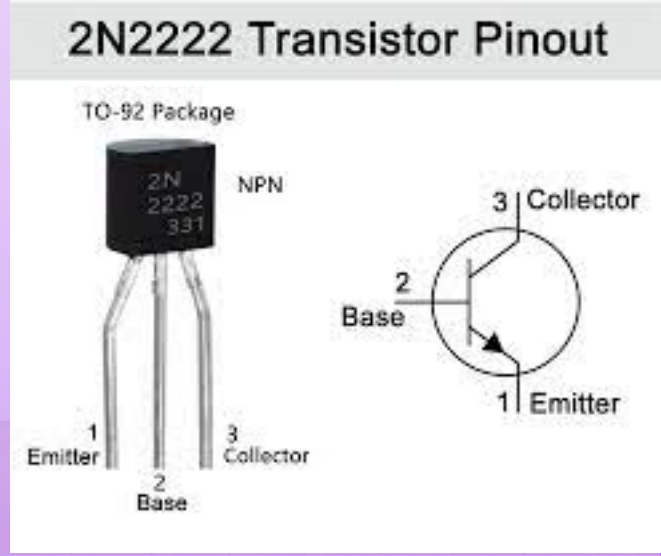
UNIVERSIDAD NACIONAL DE COLOMBIA.
DEPARTAMENTO DE FISICA

SEDE BOGOTA

28/02/2026



- **Litografía de chip:** miles y miles de transistores de escala nano-métrica.
- Los transistores son pequeños interruptores que activan o desactivan la corriente eléctrica
- AL reducir el tamaño de los transistores, aumentan la capacidad de cómputo del chip.
- Un **microchip es un conjunto de circuitos electrónicos** en una pequeña pastilla de **silicio.**
- El silicio es el segundo elemento más abundante en la Tierra.
- La invención del transistor fue entre el 1947 y el 1948 por
- John Bardeen, Walter Houser Brattain y William Shockley.
- https://youtu.be/f3IUVvJ2XgI?si=JKzYGhLIkfzwC9V9

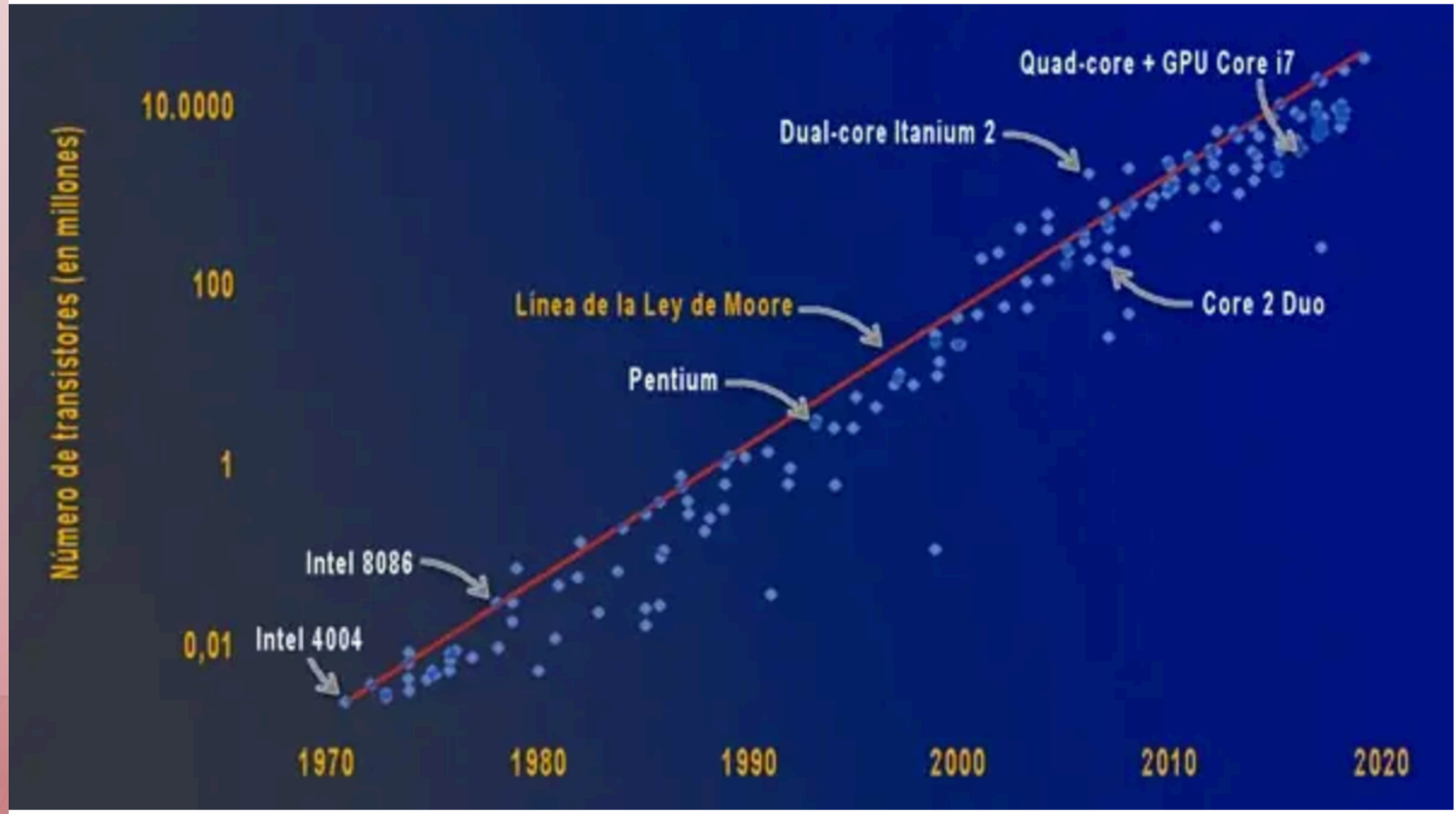


- Un nano-metro equivale a una mil millonésima parte de un metro.
- 10^-3 x10^-6 mt =10^-9 mt.
- Hoy se usan nanochips de 3 nm.
- **IBM puede meter 50.000 millones de transistores en "un chip del tamaño de una uña".**
- **La guerra de los chips. CHINA – TAIWAN. Cris Miller**
- Afecta producción de carros, teléfonos inteligentes, tarjetas gráficas, juegos, inteligencia artificial. Nvidia (chatGPT) vs DeepSeek.
- Los principales fabricantes de chips comerciales como **IBM, Intel y TSMC** "producen chips de 2 nm".
- https://youtu.be/zAYCfw_syFc?si=n6oYcS9ePh2_GeXi. ASML

LEY DE MOORE

- Duplicar el # de transistores por año.
- Límite el tamaño atómico
- Efecto túnel
- Calor generado
- **Graphcore MK2.**
- **IBM (2021)**

60.000 millones de Transistores.



SISTEMA BINARIO Y DECIMAL

La **computadora clásica** usa bits de datos { 0, 1}.

Los bits se representan en un circuito eléctrico como 0 voltios y un voltaje de referencia V_0: 1 voltio.

A este sistema se llama binario.

Existe un método para ir del **sistema binario** {0,1}

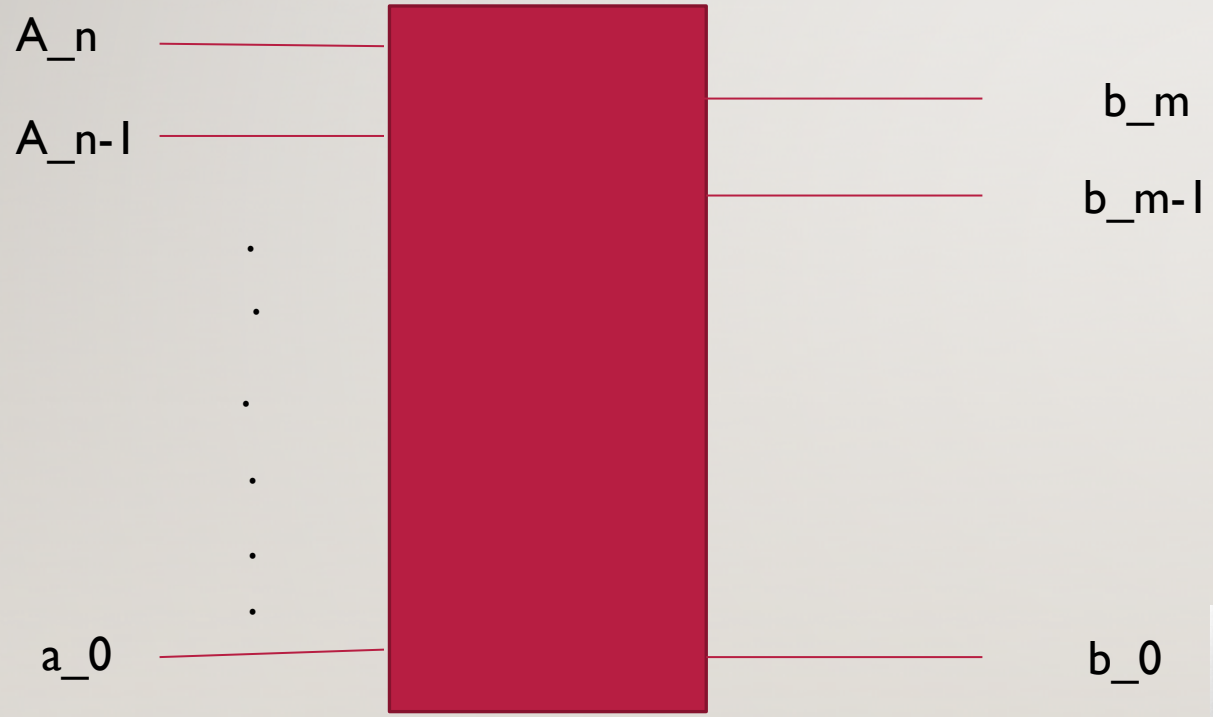
Al **sistema decimal** {0,1, 2, 3, 4, 5, 6, 7, 8, 9}.

DECIMAL: 2853 = 2 x10^3 + 8 x10^2 + 5 x10^1 + 3 x10^0

2853 = (2, 8, 5, 3)

- BINARIO:
- 65= 1 x 2^6 + 0 x 2^5 + 0 x 2^4 + 0 x 2^3 + 0 x 2^2 + 0 x 2^1+ 1 x 2^0
- 65 = 64 + 0 + 0 + 0 + 0 + 0 + 1
- 65 Requiere 6 bits (a_6, a_5, a_4, a_3, a_2, a_1, a_0)
- 65 = (1, 0, 0, 0, 0, 0, 1)

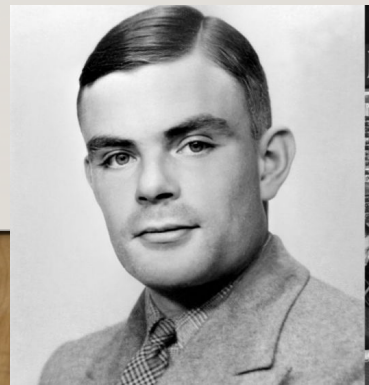
- F es una función de Boole que representa un algoritmo para un computador o maquina de Turing.
- Pregunta: Todo problema matemático se puede resolver con un algoritmo i.e. resolver mediante una maquina de Turing?

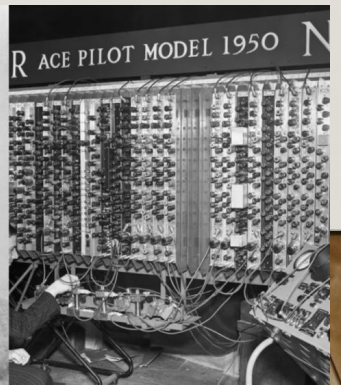


$$F : \{0,1\}^n \rightarrow \{0,1\}^m$$

$$A=(a_{n-1}, \ldots, a_i, \ldots, a_0)$$
$$B=(b_{m-1}, \ldots, b_i, \ldots, b_0)$$

Turing





Goedel

NOT

A	$\bar{A}$
1	0

OR

A	B	A ∨ B
0	0	0
0	1	1
1	0	1
1	1	1

AND

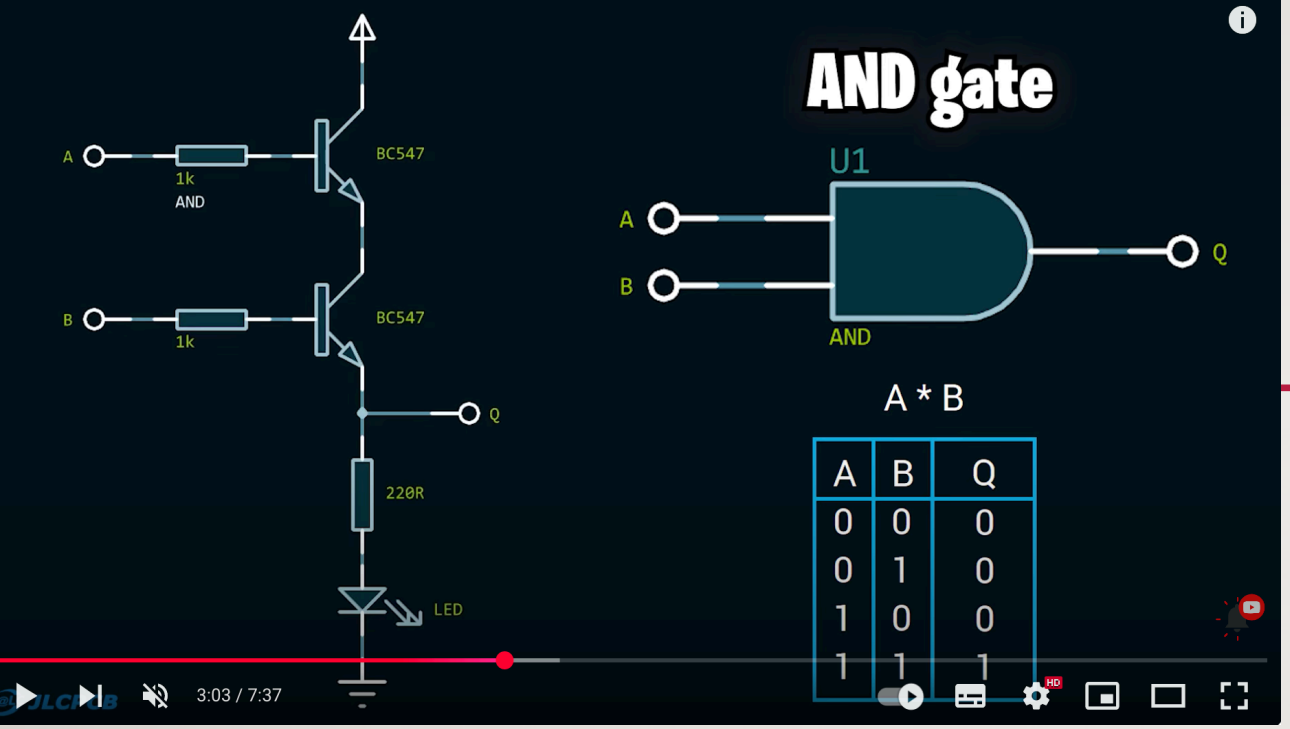
A	B	A ∧ B
0	0	0
0	1	0
1	0	0
1	1	1

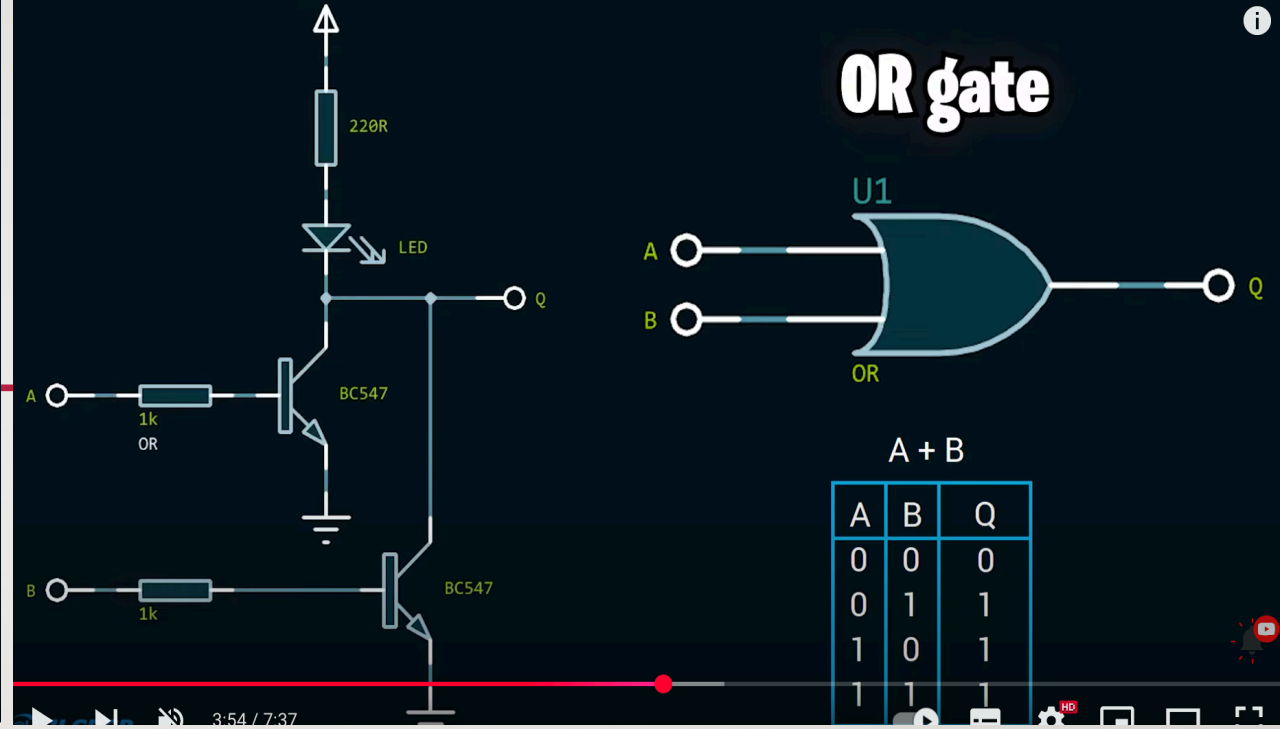
{AND, OR, NOT} se conocen como las **compuertas universales** de la computación clásica.

Cualquier algoritmo que se ejecuta en un computador o maquina de Turing se representa mediante una función F de Boole.

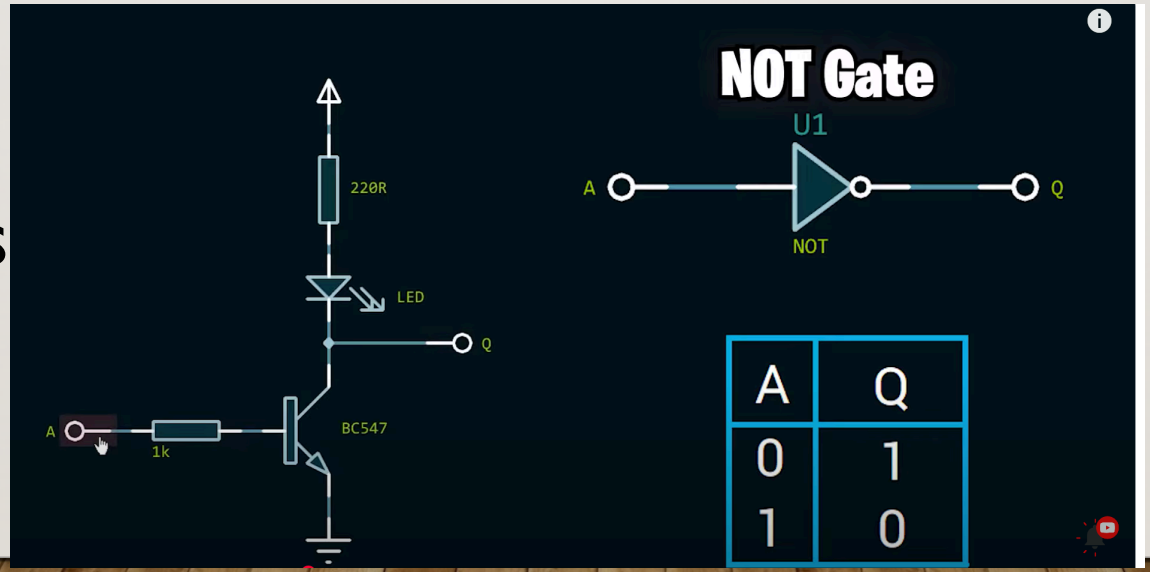
Cualquier función de Boole se puede escribir usando únicamente

{NOT, OR, AND}





Gates o compuertas fundamentales



AND

OR

NOT

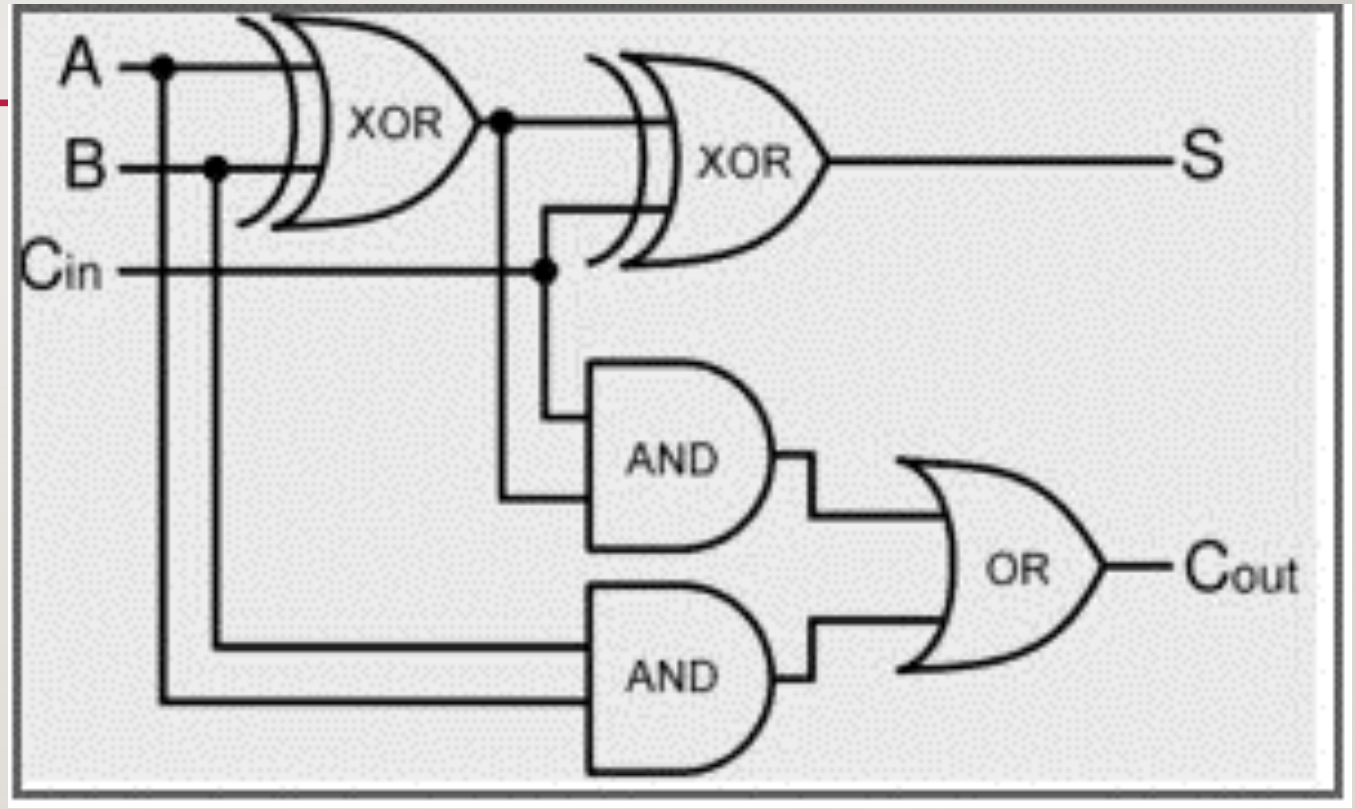
SUMADOR CON UN COMPUTADOS CLASICO

Sumador para 2 bits

A=$(a_{n-1}, \dots, a_i, \dots, a_0)$
B=$(b_{n-1}, \dots, b_i, \dots, b_0)$

$$S_i = a_i \oplus b_i \oplus c_i$$

$$C_{i+1} = (a_i \wedge b_i) \oplus (a_i \wedge c_i) \oplus (b_i \wedge c_i)$$



2+2=4

	1	0
	1	0
1	0	0

AND se denota $\wedge$
XOR se denota $\oplus$

$1 \oplus 1 = 0$ *decimos llevamos* 1, *corresponde a* c_2

COMPUTACIÓN CUÁNTICA

- *Todo lo dicho en la **computación clásica** vale*

Para la **computación cuántica**.

- Se cambia el **bit** por **qubit.**

- **Adicionalmente:**

1. **Principio de superposición**
2. **Entrelazamiento cuántico**

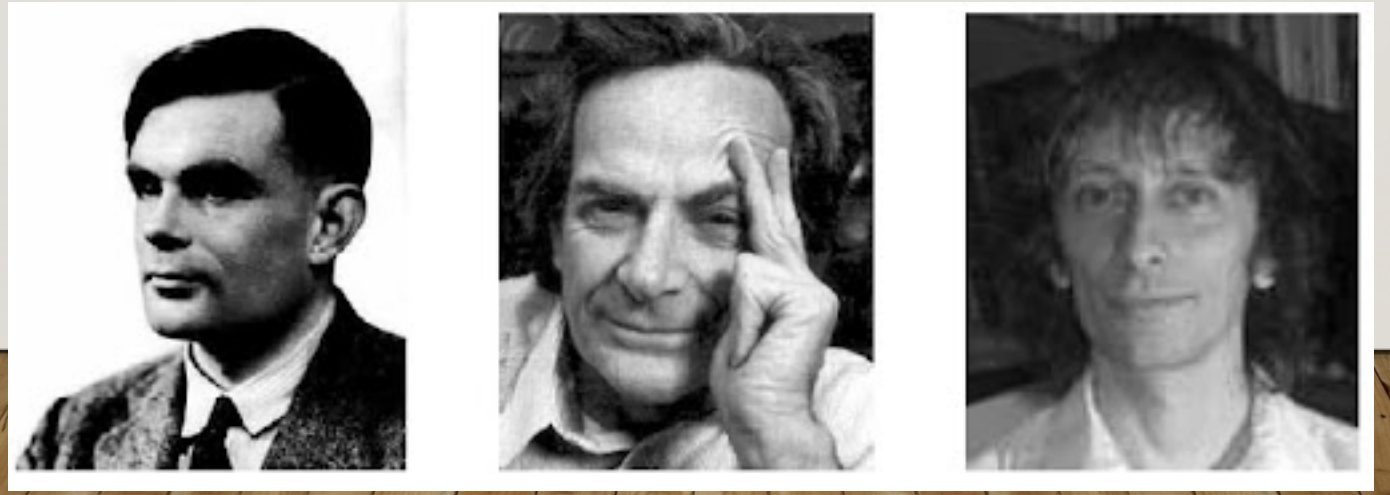
La idea de la **computación cuántica** fue introducida por primera vez en 1982, por Richard Feyman debido al límite atómico para seguir disminuyendo el tamaño de los transistores.

Las ideas esenciales de la computación cuántica surgieron de la mente de Paul Benioff. Imaginó un ordenador tradicional (máquina de Turing) que trabajaba con algunos principios de la mecánica cuántica. Argonne

El padre de la computación cuántica fue l físico de Oxford David Deutsch inventó la computación cuántica para demostrar la existencia de universos paralelos

Feynman

Deutsch



Benioff

SUPREMACÍA CUÁNTICA

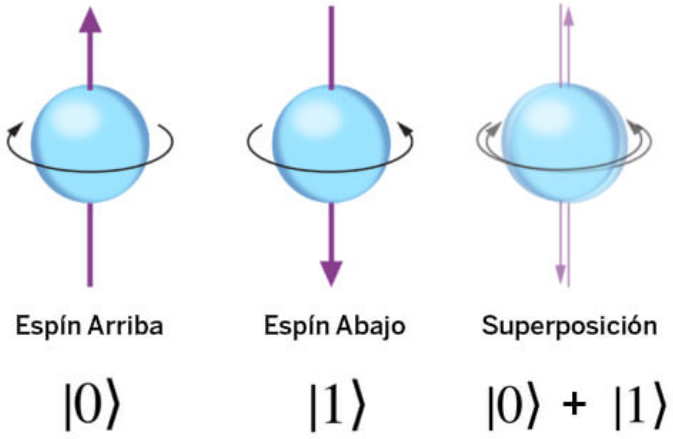
- Cuando una computadora cuántica pueda resolver un problema de la computadora clásica que no puede hacer en un tiempo razonable.
- Google anuncio supremacía cuántica con su procesador cuántico Sycamore. La tarea la hicieron en 3 minutos, en cambio un clásico podría tardar 10.000 años.
- IBM no estuvieron de acuerdo. Se corrigió el algoritmo clásico y tardó 2.5 días

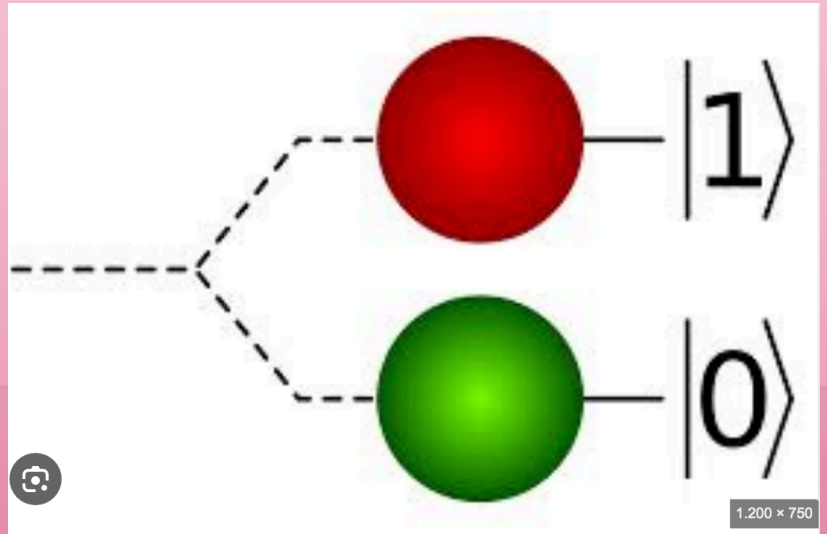
La **computación cuántica** utiliza estados cuánticos: QUBITS

Spin, fotones polarizados, atomos de 2 niveles, juntura Josephson.

$|\uparrow> = |0>, \qquad |\downarrow> = |1>$

- La computadora cuántica utiliza una propiedad cuántica llamada superposición de estados.
- $$\Psi = \alpha\,|0> + \beta\,|1>$$





PROBLEMAS COMPUTADOR CUÁNTICO

Si no está aislado se pierde la coherencia cuántica.

- Es decir colapsa la función de onda al estado |0> o |1>.
- También podría cambiar el estado cuántico por la aparición de una fase

$$\Psi = \alpha\,|0> + \beta e^{i\delta}|1>$$

• ERRORES DE DECOHERENCIA

- Problema principal de la computación cuántica es la decoherencia cuántica. Colapsa la función de onda y los pasos del algoritmo cuántico.
- Los tiempos de decoherencia está entre nanosegundos y segundos, a temperaturas bajas.
- Las tasas de error son proporcionales a la razón entre tiempo de operación frente a tiempo de decoherencia.
- La operación debe demorar un tiempo mucho más corto que el tiempo de decoherencia.
- Si la tasa de error es lo bastante baja, es posible usar corrección cuántica de errores.
- Algoritmos cuánticos que permiten saber si hubo o no de decoherencia, un error cuántico. En algunos casos hay que introducir 3 o 5 veces mas qubits para el

COMPUTACION CUANTICA. EMPRESAS

- **1. IBM Quantum**IBM es una de las pioneras en el desarrollo de hardware y software cuántico. Sus procesadores cuánticos basados en superconductores han permitido avances significativos en la investigación académica y empresarial.
- **2. Google Quantum AI** ha sido protagonista en el campo cuántico desde su demostración de **supremacía cuántica en 2019** con su procesador **Sycamore**.
- **3. Microsoft Quantum** ha desarrollado **Azure Quantum**. Además, su investigación en **qubits topológicos** busca mejorar la estabilidad de los sistemas cuánticos, una de las principales barreras para su adopción comercial.
- **4. Intel Quantum Computing** apuesta por el desarrollo de **qubits de spin de silicio**, aprovechando su experiencia en la fabricación de semiconductores.
- **5. D-Wave Systems** se especializa en **computación cuántica adiabática**, una tecnología especialmente eficaz para problemas de optimización y machine learning.

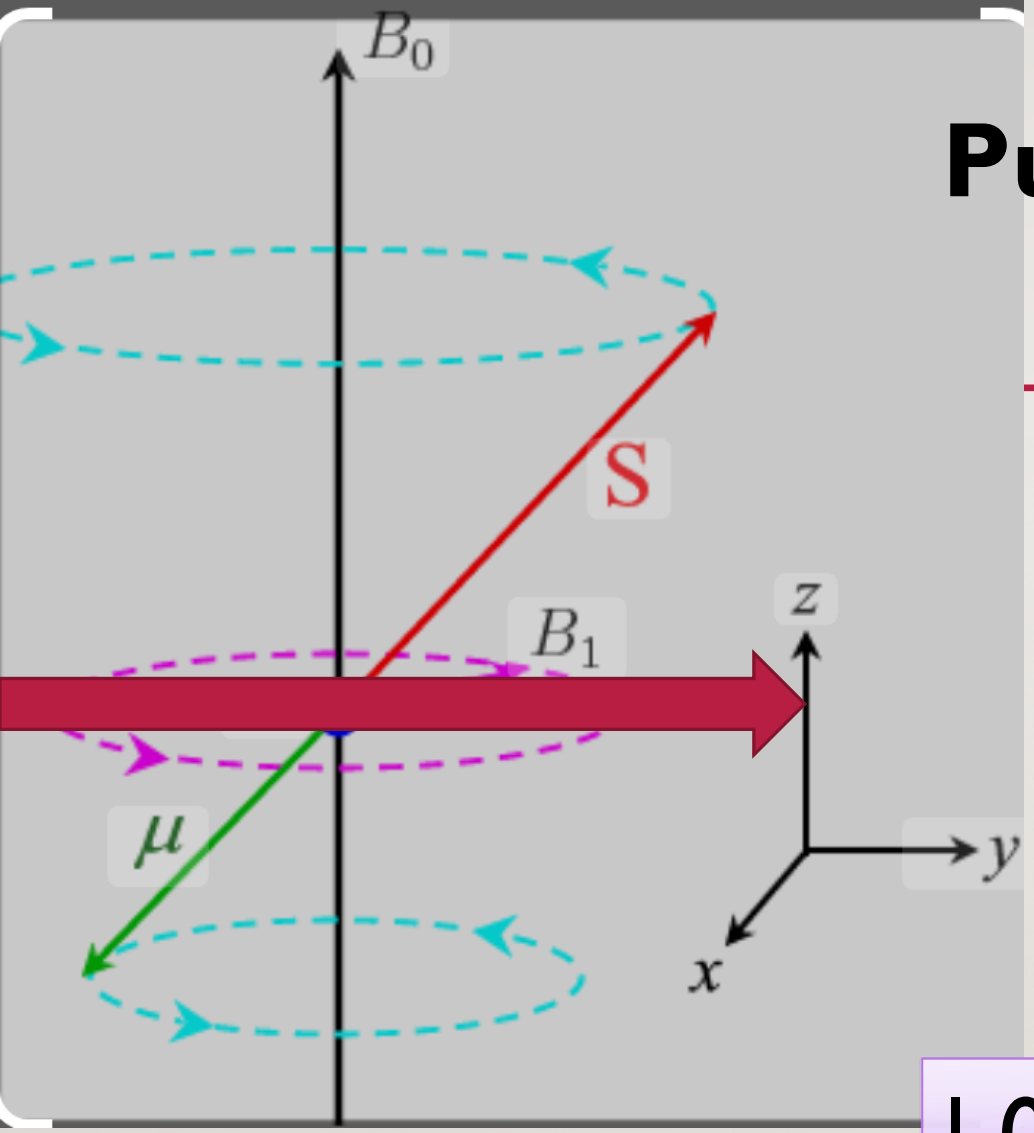
- **6. Rigetti Computing** desarrolla procesadores cuánticos superconductores con un enfoque en plataformas **híbridas**, que combinan computación cuántica y clásica.
- **7. Alibaba Quantum Laboratory (AQL)** ha entrado en el mundo de la computación cuántica con investigación en **criptografía cuántica** y modelos cuánticos para aplicaciones comerciales.
- **8. Honeywell Quantum Solutions** desarrolla ordenadores cuánticos basados en **iones atrapados**. Su enfoque está en aplicaciones de **química cuántica y simulaciones avanzadas**. Por lo tanto, su estrategia apunta a consolidar su liderazgo en sectores clave como la industria química y la farmacéutica.
- **9. IonQ** se especializa en sistemas cuánticos de **iones atrapados** y colabora con plataformas como **Microsoft Azure Quantum y Amazon Braket** . Su principal objetivo es el desarrollo de arquitecturas escalables para resolver problemas en sectores como la sanidad y las finanzas.
- **10. PsiQuantum** usa **computación cuántica fotónica**. Utiliza tecnologías de semiconductores. Aplica estos sistemas en **Inteligencia artificial y modelado molecular**.

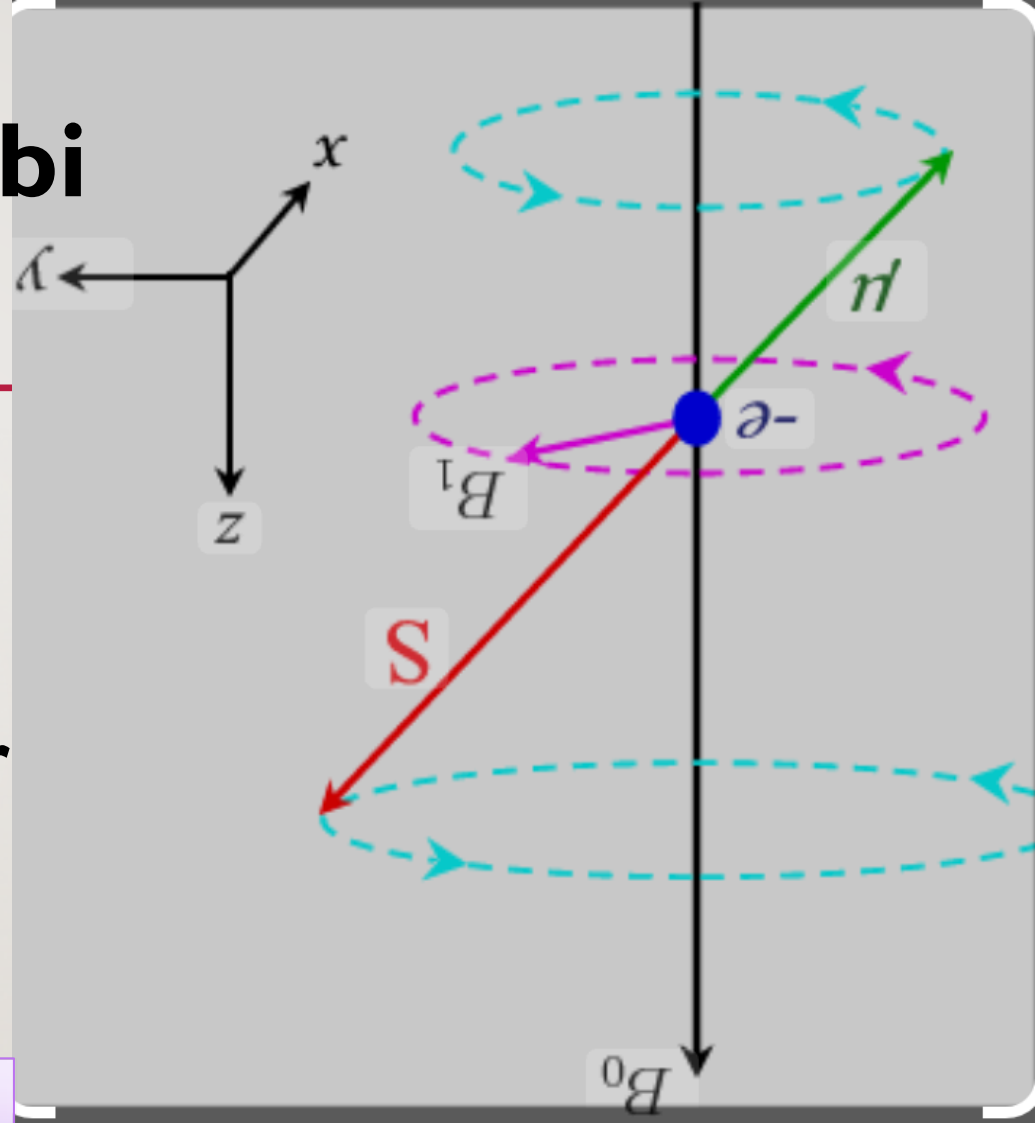

NVIDIA
Google

Pulso de Rabi

Nobel

Alumno de Oppenheimer





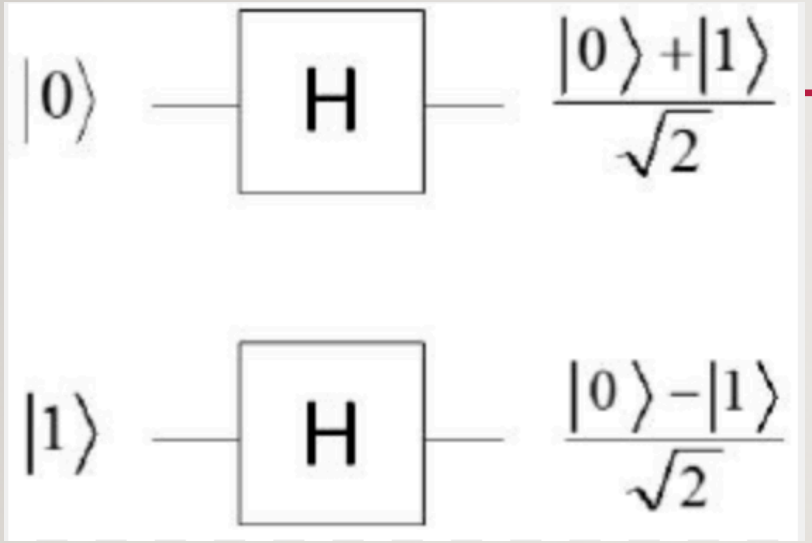
$| 0 > + | 1 >$

$| 0 >$

$| 0 > - | 1 >$

$| 1 >$

GATES O COMPUERTAS CUÁNTICAS. HADAMARD



$n = 2$

$$H \otimes H|00\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) =$$

$$= \frac{1}{2}(|00\rangle + |10\rangle + |01\rangle + |11\rangle) =$$

$$= \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle)$$

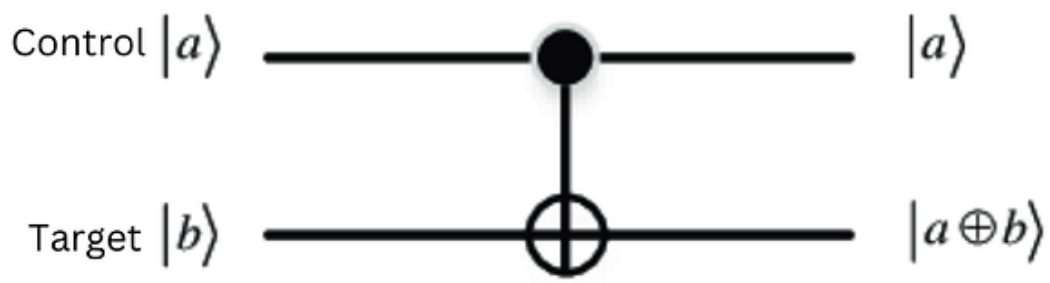
$|00> = |0> \otimes |0>$

Al aplicar H⊗H al estado |00> obtenemos la **superposición** de todos los estados cuanticos de 2 qubits :

|00>+|01>+|10>+|11>.

OTRAS COMPUERTAS
CONTROL NOT (CNOT)

$$\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

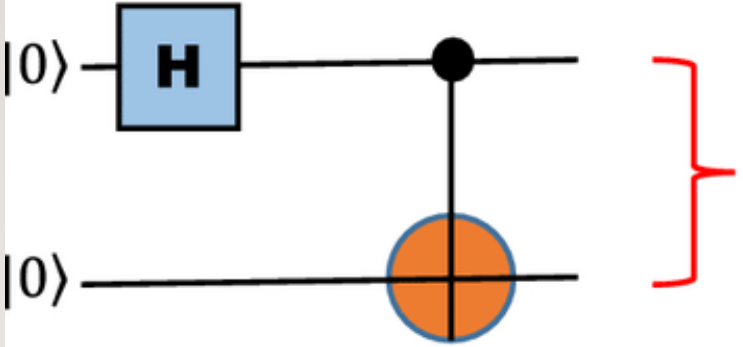


Si |a>=|0> entonces el target |b> NO CAMBIA

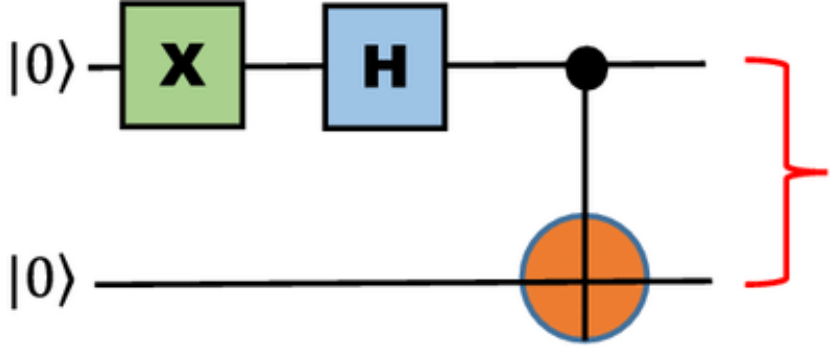
Si |a>=|1 > entonces el target $|1 \oplus b >$ = $|\overline{b} >$ CAMBIA

BASE DE BELL

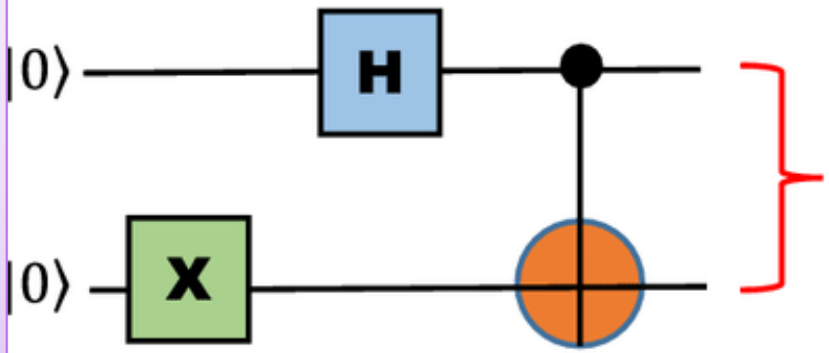
ESTADOS ENTRELAZADOS



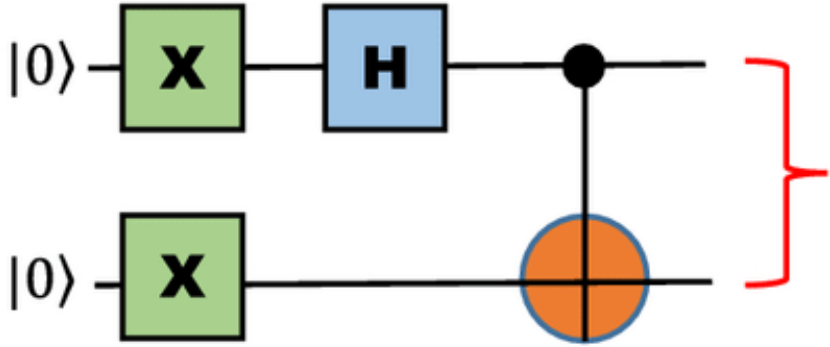
$$|\psi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$



$$|\psi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

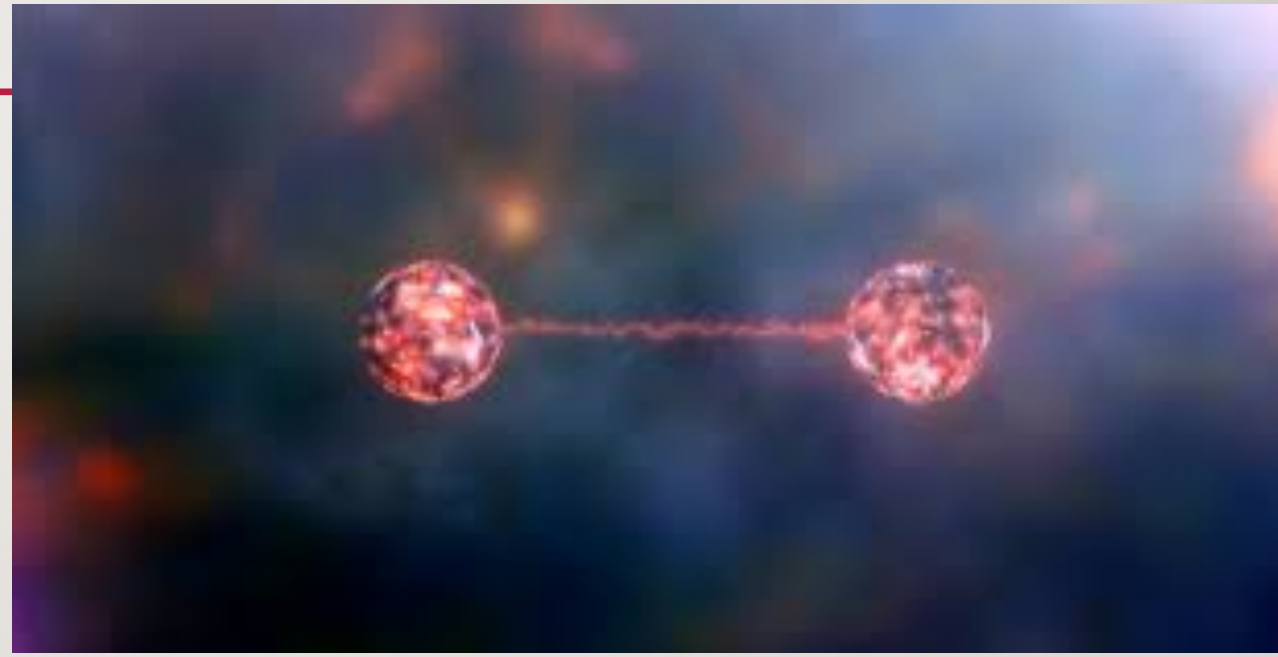


$$|\phi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$



$$|\phi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

ENTRELAZAMIENTO CUANTICO
ENTANGLEMENT



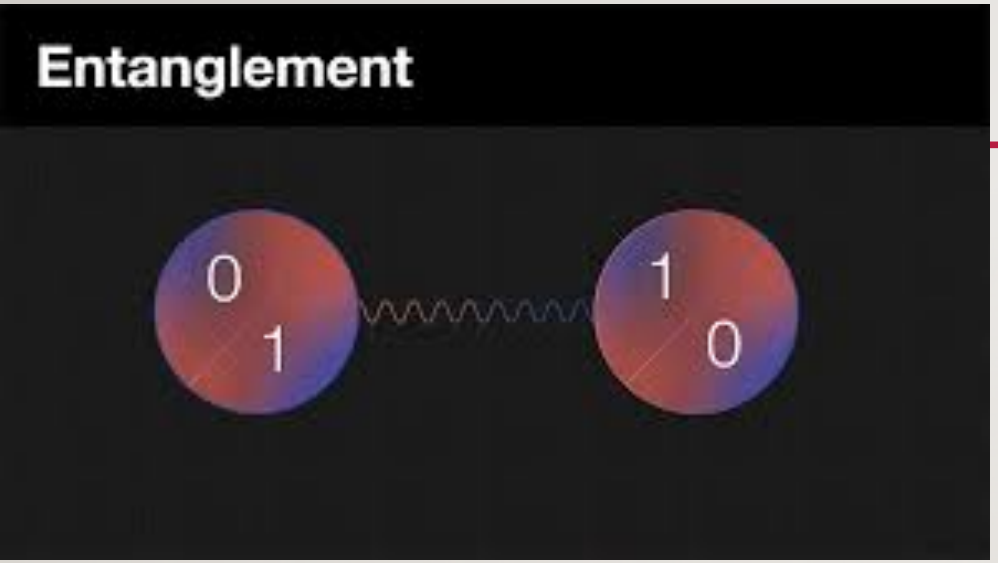
Albert Einstein, Boris Podolski y Nathan Rosen cuestionaron las bases de la MQ en 1935

Sus aportaciones demostraron experimentalmente

- El entrelazamiento,
- Violaciones de las desigualdades de Bell
- La teletransportación cuántica.

ASPECT – CLAUSER – ZEILING.
NOBEL 2022

ENTRELAZAMIENTO CUANTICO



Su estado cuántico se describe como

$$|\Psi> = c_1\,|01> \; + c_2\,|10>$$

$$= c_1\,|0> \otimes |1> + c_2 |1> \otimes |0>$$

$$= c_1\,|\uparrow> \otimes \quad |\downarrow> + c_2 |\downarrow> \otimes \quad |\uparrow>$$

Dos electrones con sus espines arriba |0> o abajo |1>.

Remotamente separados

Tierra Sol

$$c_1 |\uparrow\downarrow> e_1 \otimes |\downarrow\uparrow> e_2 \;+\; c_2 |\downarrow\uparrow> e_1 \otimes |\uparrow\downarrow> e_2$$

- Si medimos sobre e_1 en la TIERRA y encontramos que está $\uparrow$ la función de onda COLAPSA

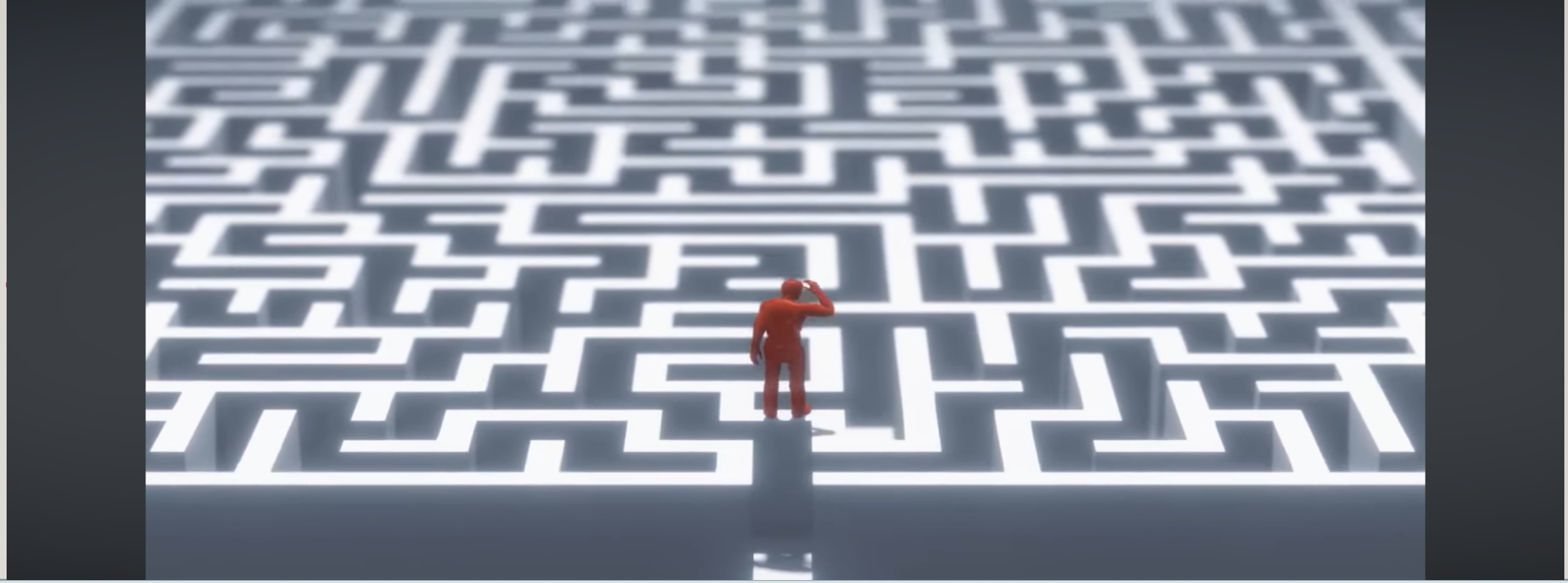
- $$|\uparrow\downarrow> e_1 \quad \otimes \quad |\downarrow\uparrow> e_2$$

- Entonces el electrón en el SOL e_2 tendrá spín $\downarrow$

Si medimos sobre e_1 en la TIERRA y encontramos que está $\downarrow$ la función de onda COLAPSA

$$|\downarrow\uparrow> e_1 \quad \otimes \quad |\uparrow\downarrow> e_2$$

El electrón en el SOL e_2 tendrá spín $\uparrow$



Para un computador clásico se necesita hacer 4 corridas para introducir toda la base de 2 bits al ORACLE {|00>, |01>, |10>, |11>}.

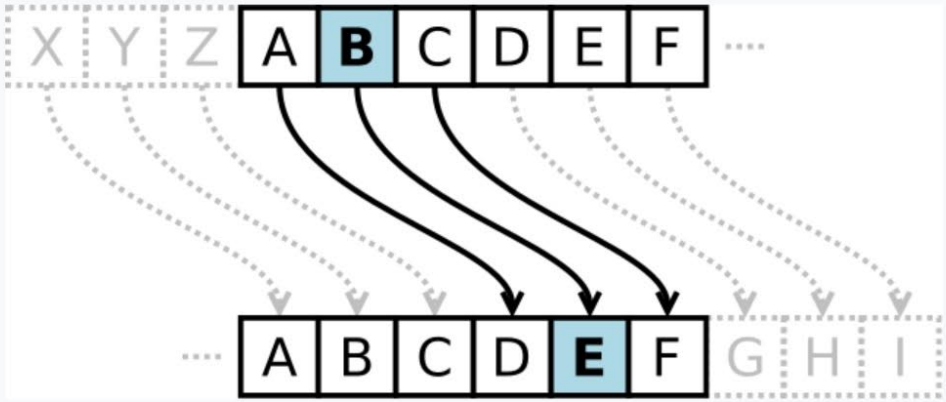
Para un computador cuántico solo 1 corrida {|00>+|01>+ |10>,+|11>}.

Para n-qubits tenemos una base de 2^n qubits y se PUEDEN introducir al ORACLE en una sola corrida.

CRIPTOGRAFÍA

Julio Cesar y Augusto usaban este tipo de cifrado de mensajes.

Cifrado César



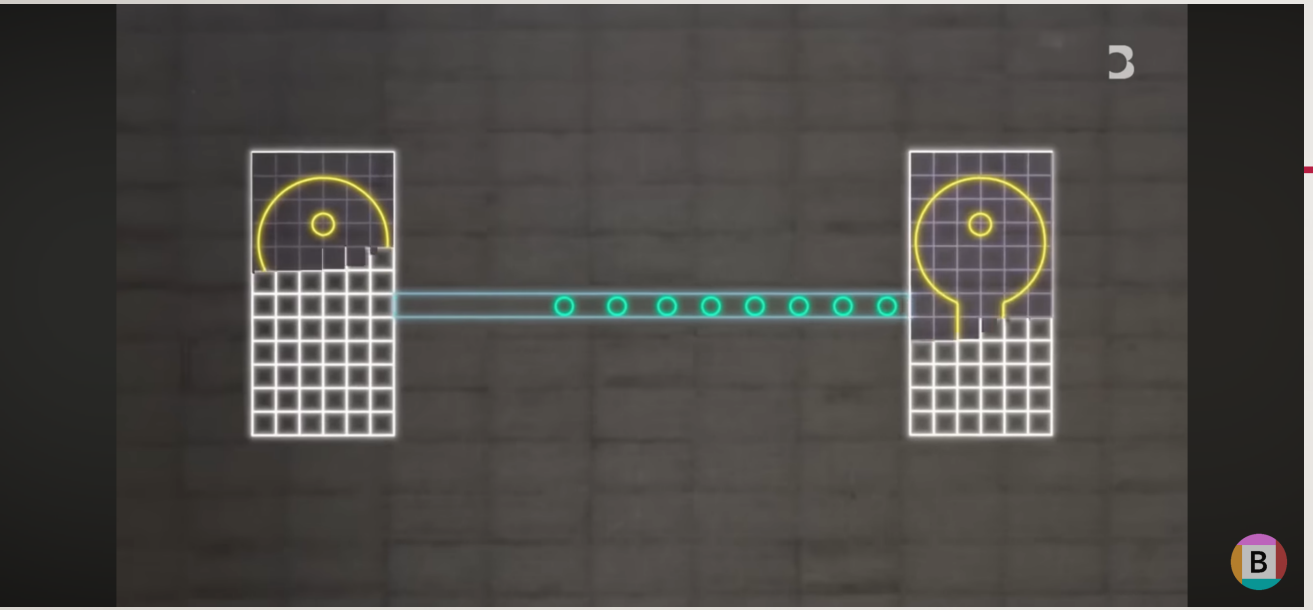
El cifrado César mueve cada letra un determinado número de espacios en el alfabeto. En este ejemplo se usa un desplazamiento de tres espacios, así que una B en el texto original se convierte en una E en el texto codificado.

derecha. Por ejemplo, aquí el cifrado César está usando un desplazamiento de seis espacios hacia la derecha:

```
Texto original:
ABCDEFGHIJKLMNÑOPQRSTUVWXYZ

Texto codificado:
GHIJKLMNÑOPQRSTUVWXYZABCDEF
```

TELE TRANSPORTACIÓN. HACKEO

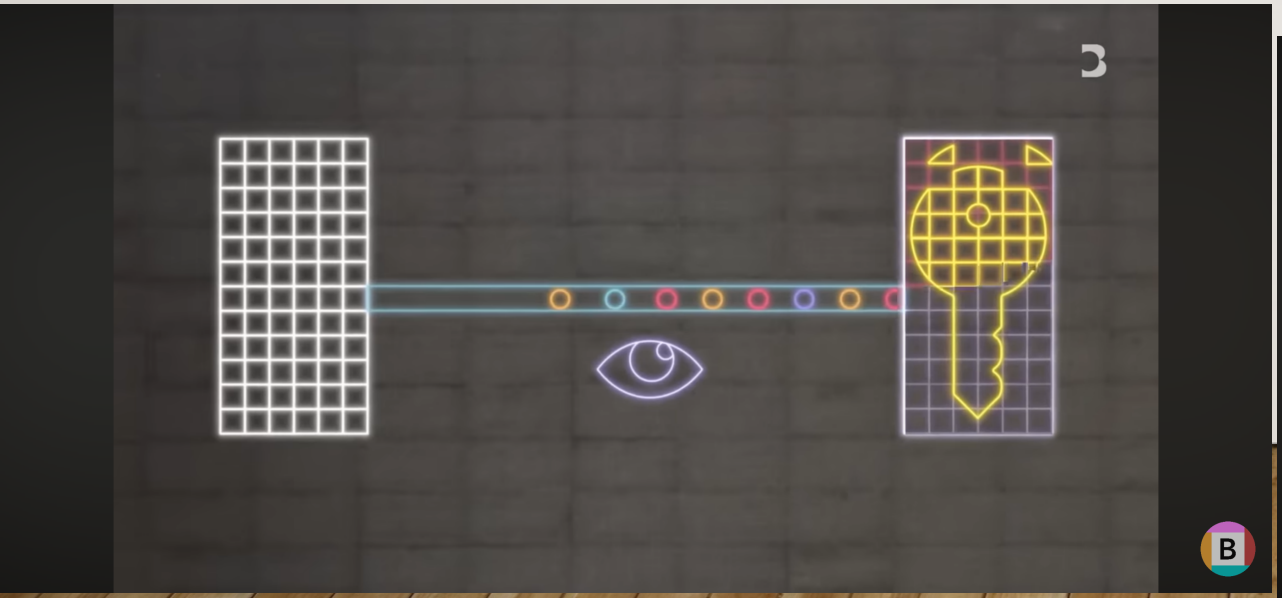


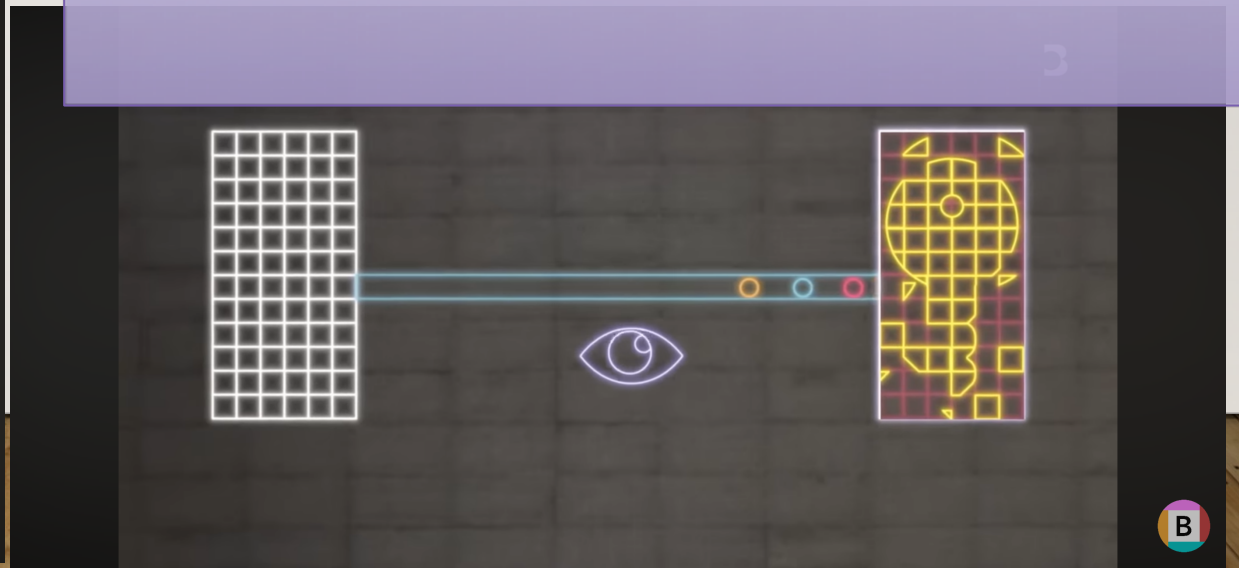
Clásicamente se envían mensajes por una fibra óptica, internet

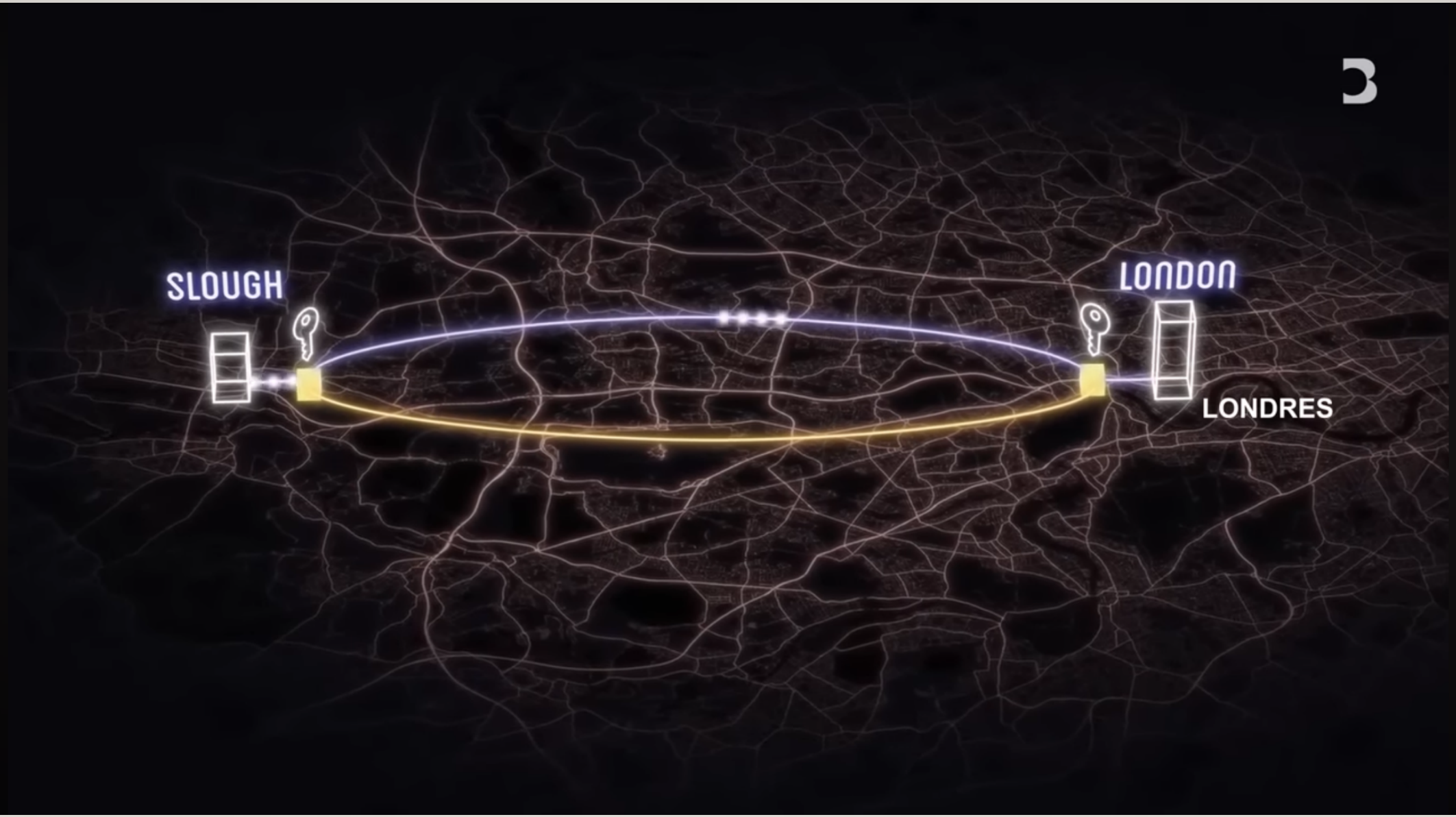
Sujeto a hackeo.

Cuántico. Se envían qbits.

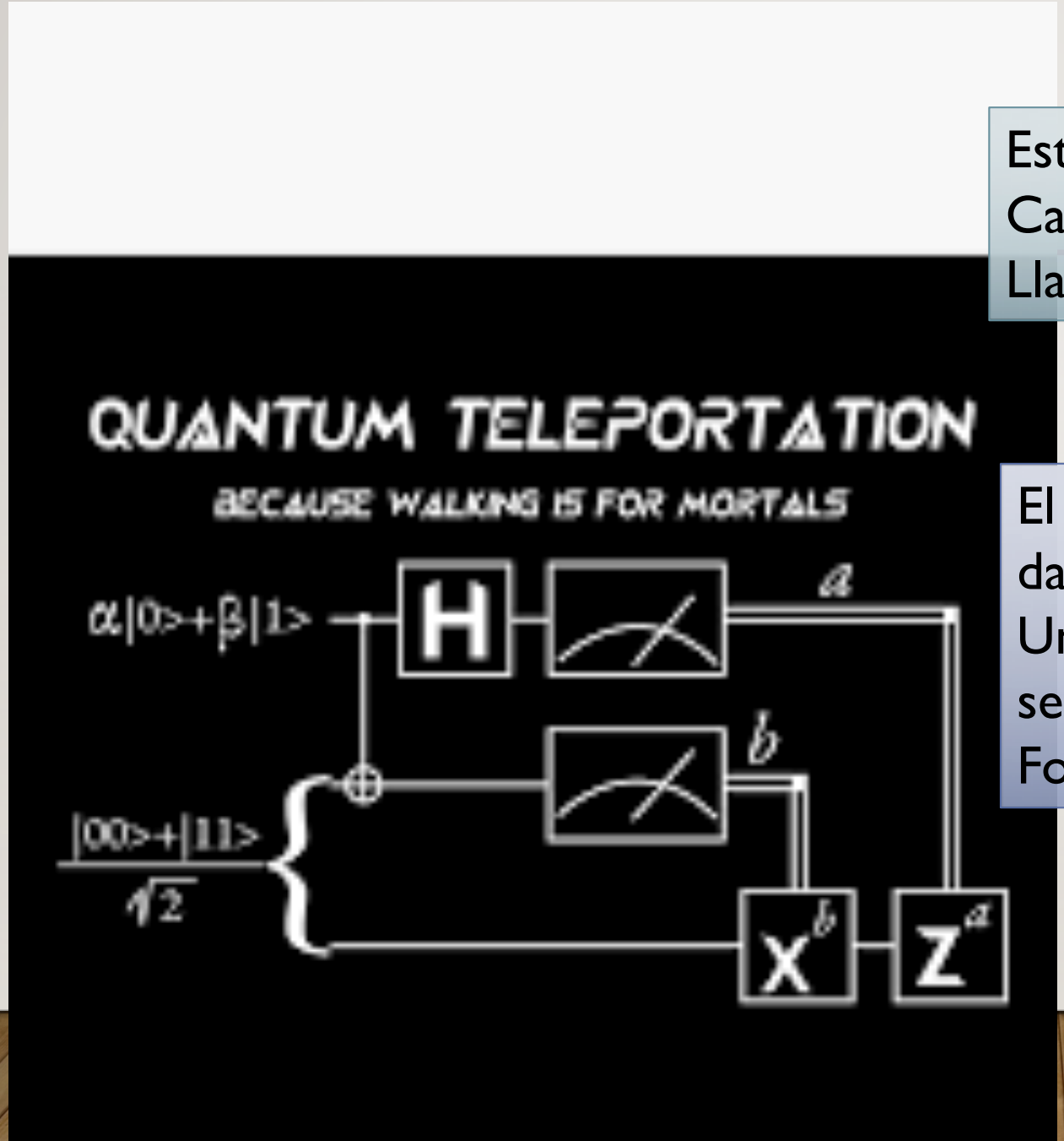
Hackeo implica colapso de los qubits






SLOUGH
LONDON
LONDRES

ALGORITMO TELE TRANSPORTACIÓN QUÁNTICA



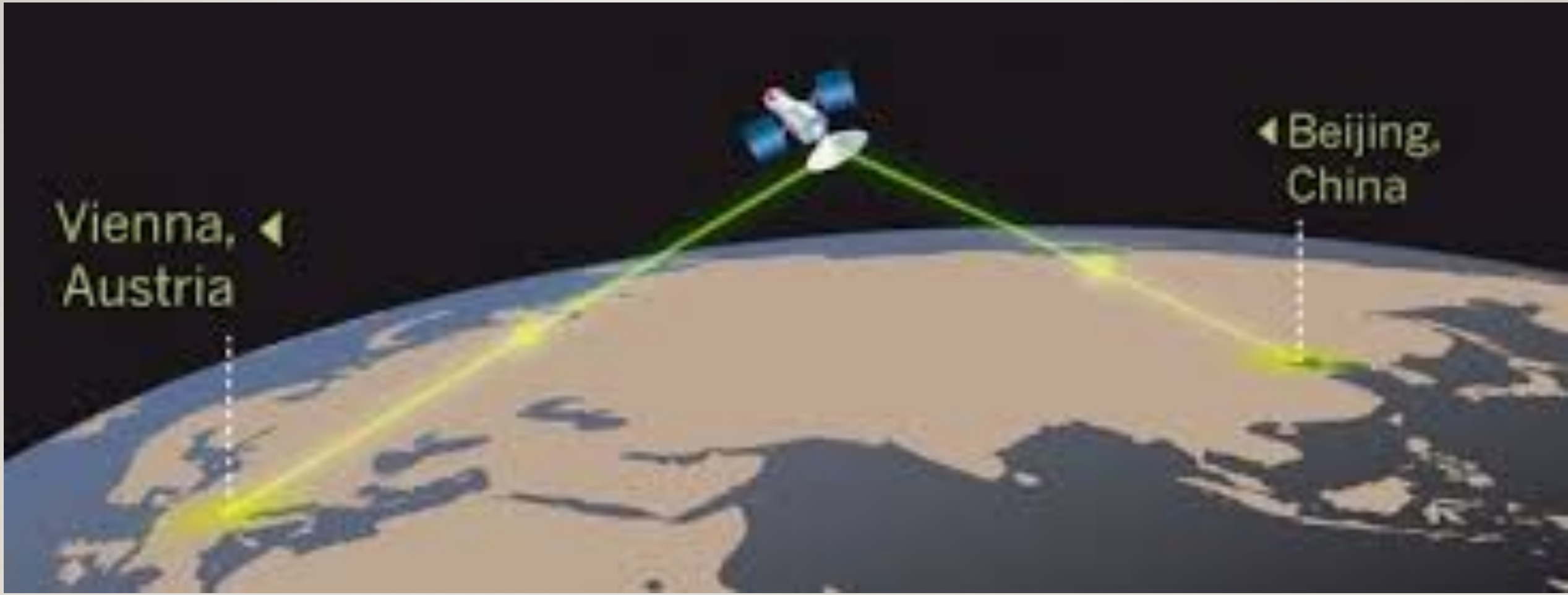
Alice

Bob

Estado entrelazado compartido Alice y Bob.
Cada uno tiene un qubit del entrelazado.
Llave

El qubit de Alice es transferido a Bob sin dañarlo.
Un hakeo colapsa la función de onda y Bob se daria cuenta.
Forma segura de enviar información

TELE TRANSPORTACIÓN QUÁNTICA
CHINOS
1200 KMS



ALGORITMO DE SHOR

CRIPTOGRAFÍA RSA: (RIVEST, SHAMIR, ADLEMAN)

- Como en todo sistema de clave pública, cada usuario posee dos claves de cifrado: una pública y otra privada. **N = pb pv**
- Cuando se quiere enviar un mensaje confidencial, el emisor busca la clave pública del receptor **(pb),** cifra su mensaje con esa clave, y una vez que el mensaje cifrado llega al receptor, este se ocupa de descifrarlo usando su clave privada **(pv).**
- Se cree que RSA será seguro mientras no se conozcan formas rápidas de descomponer un número grande **N** en producto de primos **N=pb pv**
- La computación cuántica podría proveer de una solución al problema de factorización.

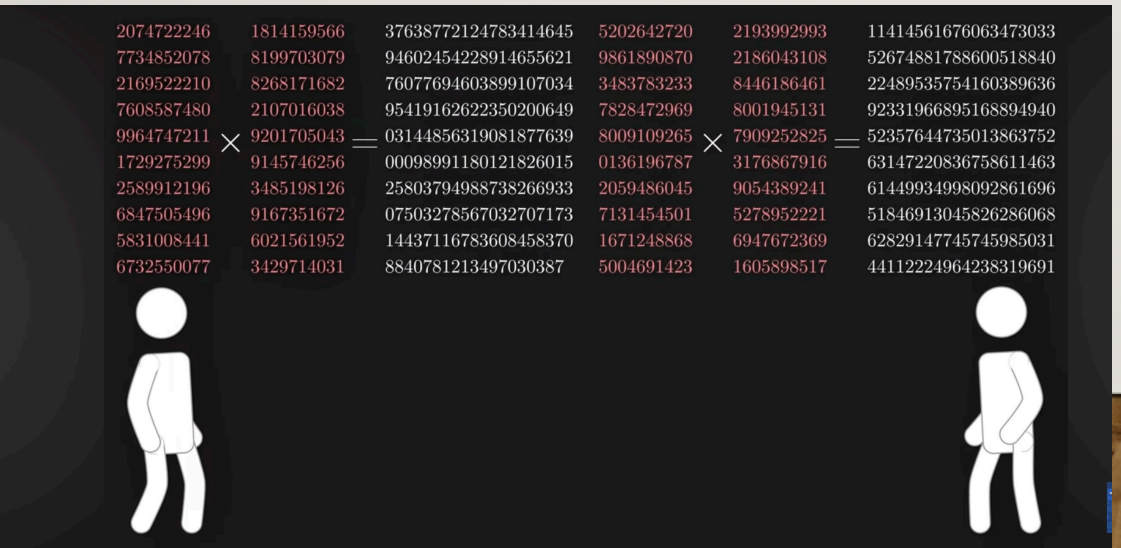
ALGORITMO DE SHOR - CRIPTOGRAFÍA

Descompone a M, N en primos
Llaves públicas y privadas

Computación cuántica puede romper la descomposición de un número en primos.

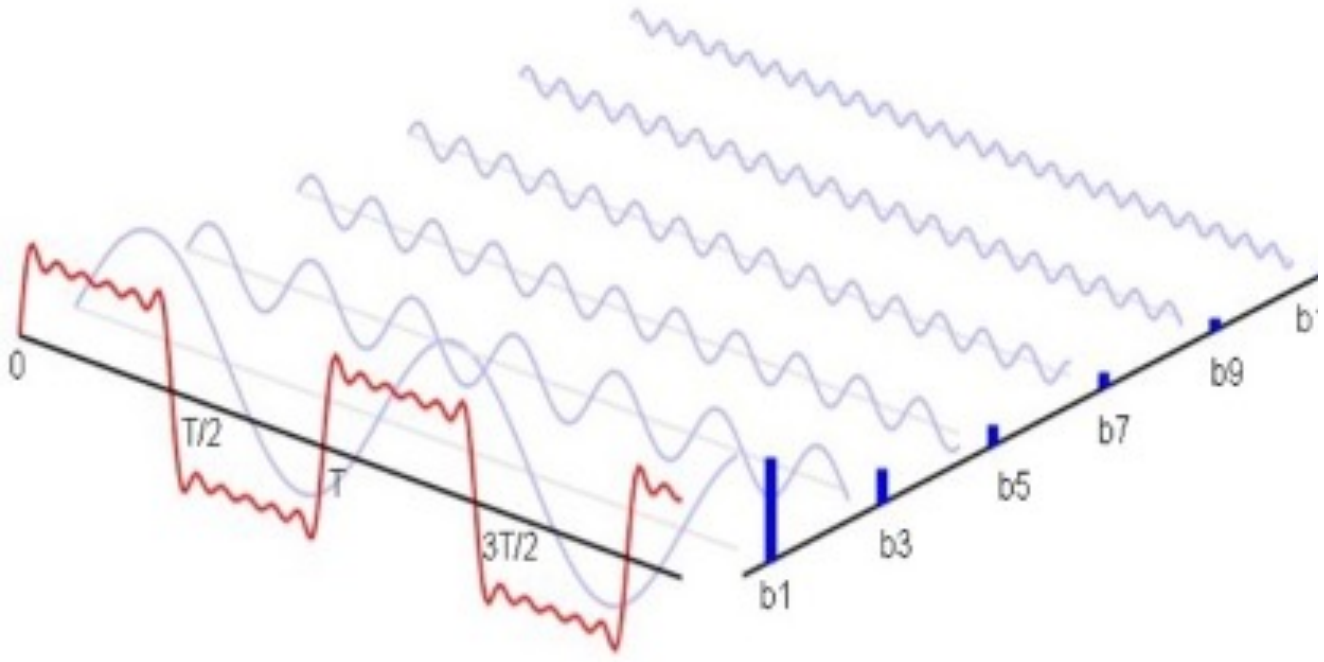
pb pv | N | pb pv | M

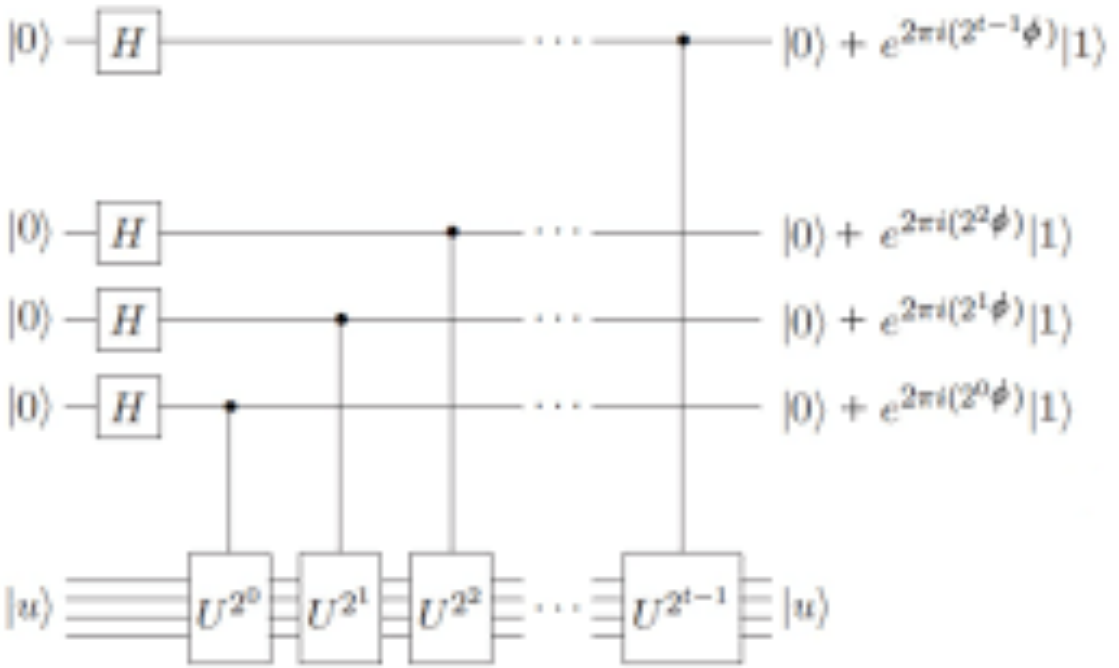
Veritasium



TRANSFORMADA QUANTICA DE FOURIER

$$U_{F_N}|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i x y/N} |y\rangle$$





COMPUERTAS QUÁNTICAS
TOFFOLI (CCN)
DE LA COMPUTACION CUANTICAUNIVERSAL

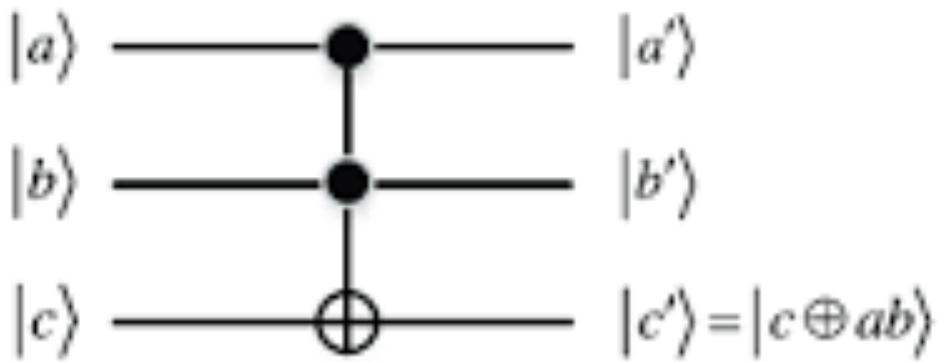
Toffoli actúa cuando los dos qubits control valen 1, |a>=|b>=1

|a.b>=1

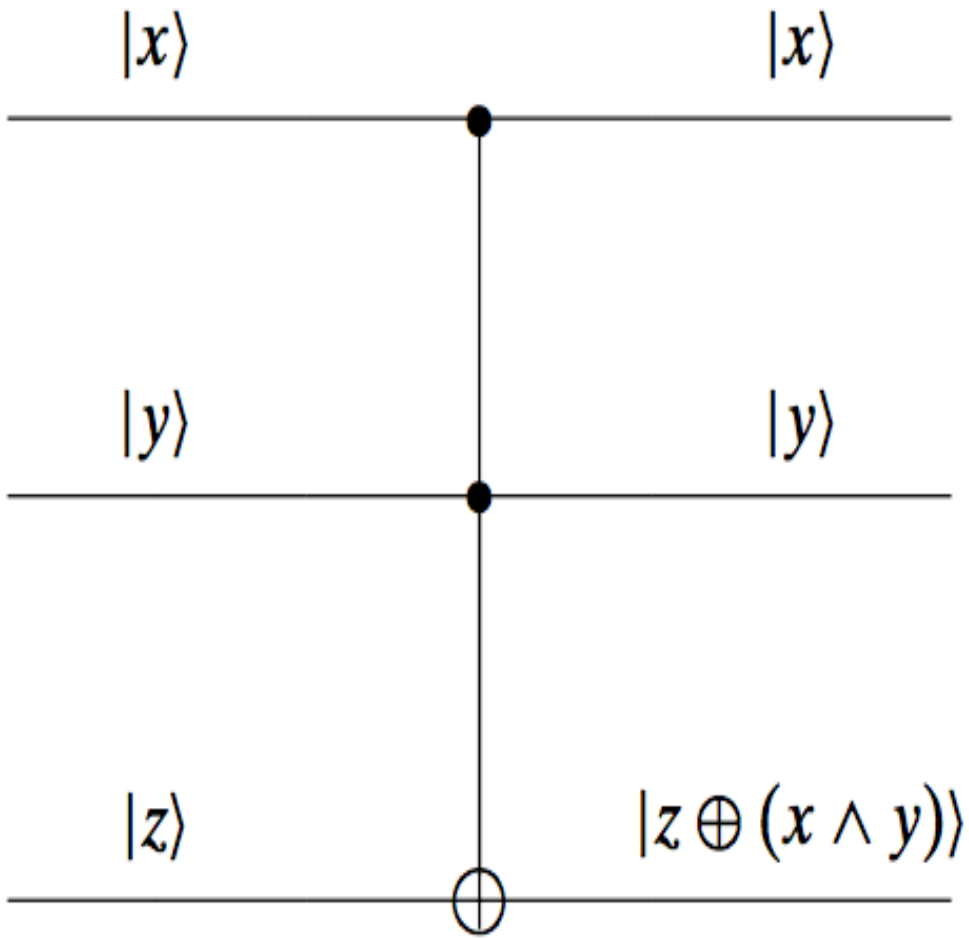
De lo contrario

|a.b>=0

Inputs			Ouputs		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0



COMPUTACIÓN UNIVERSAL
TOFFOLI (CCN)



|z>=|0> entonces $|0 \oplus x \wedge y> = |x \wedge y>$
AND

|z>=|1 > $entonces$ $|1 \oplus x \wedge y> = |\bar{x} \vee \bar{y}>$
OR

|x>=|y>=|1 > entonces $|z \oplus x \wedge y>$
$=|z \oplus 1>= |\bar{z}>$
NOT

REFERENCIAS DIVULGATIVAS

- https://youtu.be/0VV0QBSV4jY?si=ghRy7P0r7txNyBo4. Entrevista Ignacio Cirac
- https://www.youtube.com/live/hkXUsZmKUtc?si=3aasWW9Fa-g9T23q.

- https://youtu.be/ZmgIQSp6vzc?si=1vGIKOuhENPOtioR
- **Cirac construyó el primer computador con 4 qubits.**
- https://youtu.be/4D8fx1iHtpk?si=HjIQi2Uc_Kxyi_3D. Supremacía cuántica
- https://youtu.be/bfYH7JmHQnk?si=aMJP7mxpoQrrAfvR. Eduardo Saenz
- https://youtu.be/xymGpIeNc88?si=OAziu4UtOPhL9m1r. Veritasium. Encriptación
- https://youtu.be/mVu_kOtuybM?si=wsozoSSOI-4_PD2C. Fabricación de qubits
- https://youtu.be/KKwjeJzKezw?si=Gu52WDp4_45o4OMa. E. Saenz. Curso introductorio

TEMAS MAS AVANZADOS

- https://youtu.be/4BUB41iK25Y?si=yeyOOb6yHliXCJcS
- https://youtu.be/6SIX_FR4wOM?si=laeX5PD8OoLGC-MV. Algoritmo de Shor
- https://youtu.be/6SIX_FR4wOM?si=laeX5PD8OoLGC-MV. Criptografía RSA
- https://en.wikipedia.org/wiki/Qiskit
- https//quantum.ibm.com (Crear cuenta en Qiskit)