



**XIII
JORNADAS
STIC
CCN-CERT**



La amenaza de la computación cuántica: ¿hay cripto después?

**COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD**

#XIIIJORNADASCNCERT



Luis Hernández Encinas
Víctor Gayoso Martínez



Instituto de Tecnologías Físicas y de la Información (ITEFI)
Consejo Superior de Investigaciones Científicas (CSIC)

luis@iec.csic.es
victor.gayoso@iec.csic.es

Índice

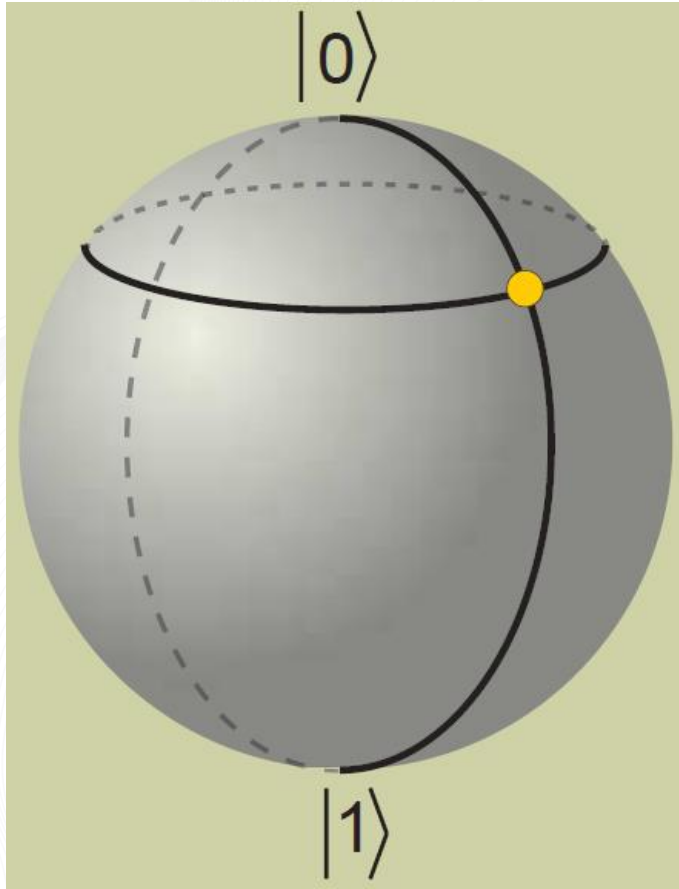
- 1. Procesamiento cuántico de la información**
- 2. Distribución cuántica de claves**
- 3. Computación cuántica**
- 4. Criptoanálisis cuánticos**
- 5. El futuro se llama criptografía postcuántica**

1. Procesamiento cuántico de la información

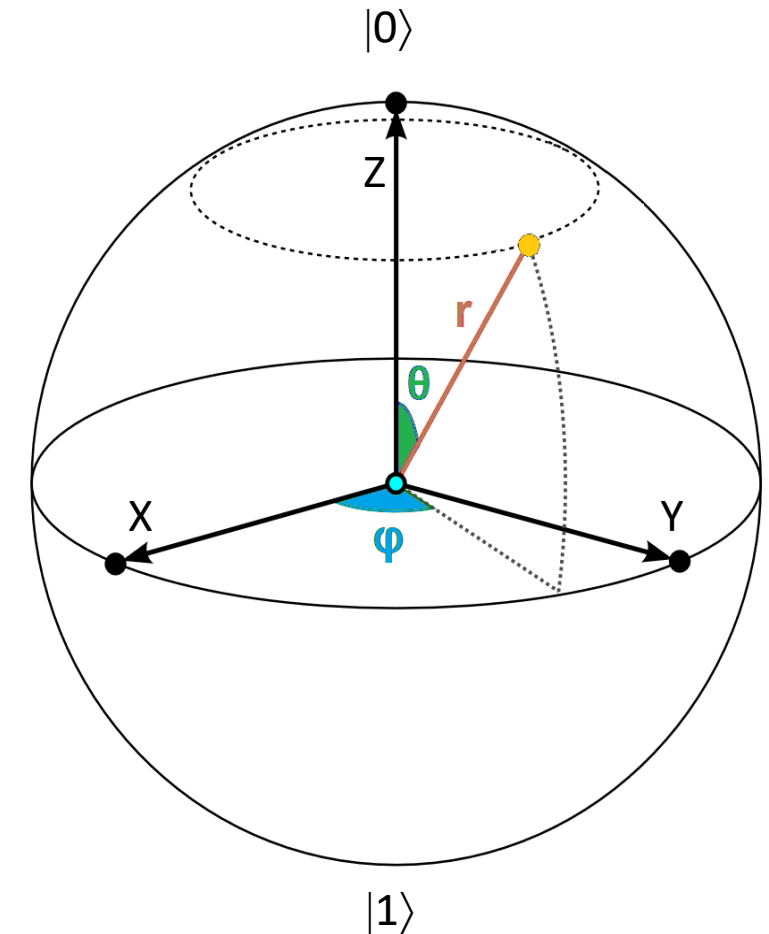
Bits clásicos y bits cuánticos

- La Mecánica cuántica es la base de la computación y la comunicación cuánticas (*Quantum Information Science*). Conviene olvidarse de los parámetros de la Física clásica y pensar *cuánticamente* (fuera de la intuición y la mecánica newtonianas).
- Los bits que codifican la información serán clásicos o cuánticos, dependiendo de los si sistemas de información y computación empleados son clásicos o cuánticos.
- Los **bits clásicos** son 0 o 1 (v.gr. un **interruptor** –apagado/encendido– codifica un bit).
- Los **bits cuánticos** (*qubits*) son $|0\rangle$ y $|1\rangle$ (se codifican con sistemas cuánticos de dos niveles, no hay interruptores) y se suelen asociar, principalmente, con el **espín de un electrón** o la **polarización de un fotón**.
- En la mecánica cuántica, un sistema cuántico que tome dos valores, también puede tomar cualquier **superposición coherente** de los dos, esto es, puede estar en el estado resultante de una combinación de $|0\rangle$ y $|1\rangle$.
- ❖ Así, por ejemplo, una posible superposición coherente podría dar lugar a que el estado del *qubit* fuera mitad $|0\rangle$ y mitad $|1\rangle$, a la vez.

Superposición coherente de estados: esfera de Bloch



- En un sistema cuántico de dos niveles, un *qubit* se puede representar como un punto en una esfera (de Bloch) de radio fijado, r .
- Los polos se asocian a los estados $|0\rangle$ y $|1\rangle$.
- Cualquier combinación (superposición) de estos dos estados da lugar a un único punto en la esfera.
- Usando coordenadas esféricas (geográficas), el *qubit* se puede determinar mediante dos ángulos: latitud (θ) y longitud (φ).



No coherencia o decoherencia

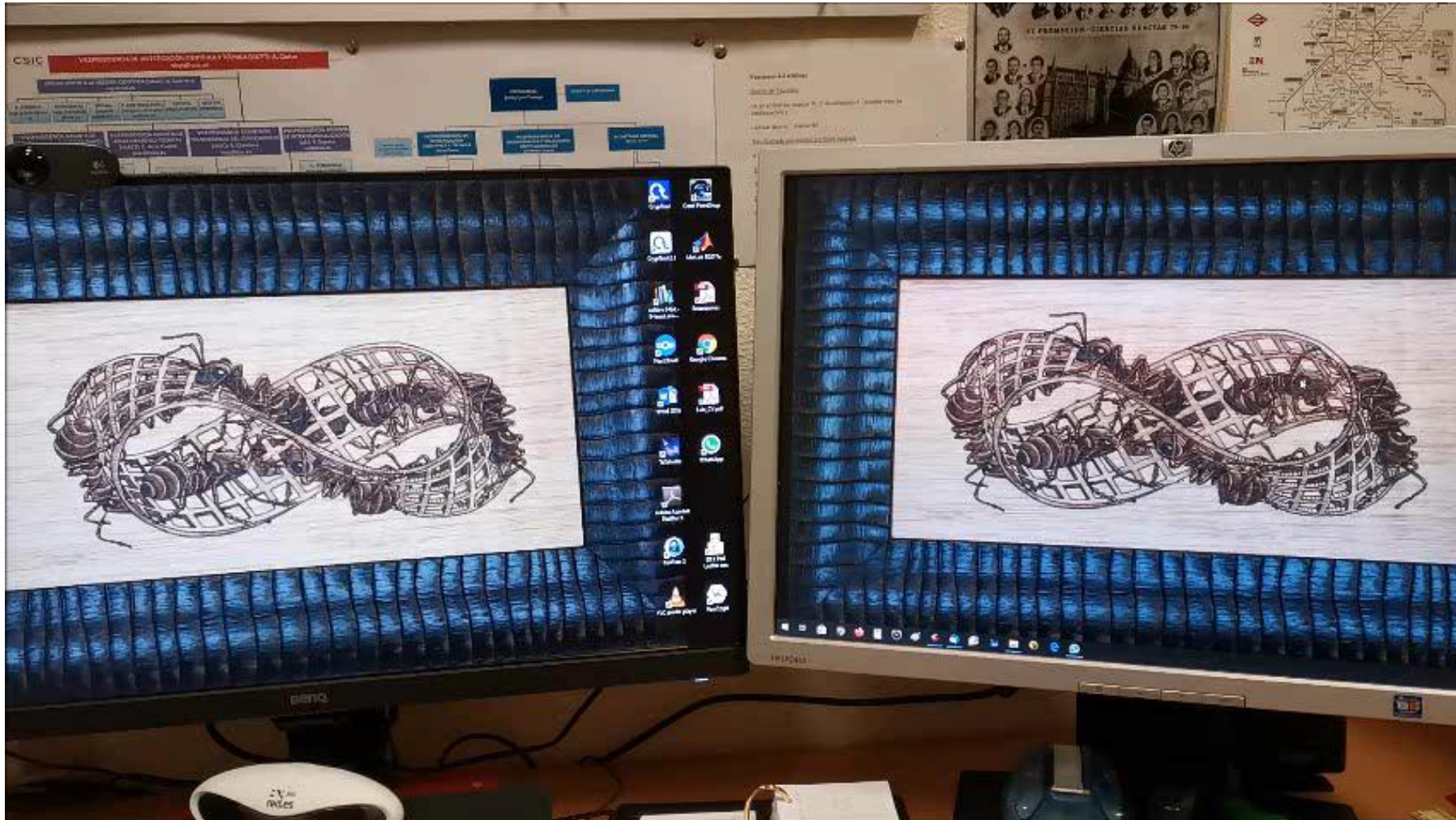
- El **Teorema de la imposibilidad de clonación** afirma que no existe una operación que produzca una copia idéntica de un estado cuántico dado y no conocido.
- El **Principio de incertidumbre (Heisenberg)** señala no se pueden medir determinados pares de variables sin cometer un error (posición y velocidad, polarizaciones no ortogonales, etc.), esto es, **medir un sistema cuántico lo altera**. Si un adversario lee una información transmitida desde un emisor a un receptor, codificada cuánticamente, la modifica y esa modificación es detectable.
- La pérdida de coherencia (**decoherencia**) producida al interactuar con el entorno hace que los dispositivos que almacenan y codifican la información pierdan sus propiedades cuánticas y entonces **se producen errores en la transmisión de la información**.
- A mayor escala, esto es, cuanto mayor sea el número de *qubits*, mayor será la tasa de error.
- La decoherencia impide la existencia de superposiciones coherentes. En entornos donde la decoherencia sea baja (aceptable), la **corrección cuántica de errores (QEC)** permite la computación cuántica o el procesamiento de la información codificada cuánticamente.
- *En situaciones reales, las correcciones de errores no son perfectas e introducen nuevo ruido.*

2. Distribución cuántica de claves (QKD)

Fotones polarizados

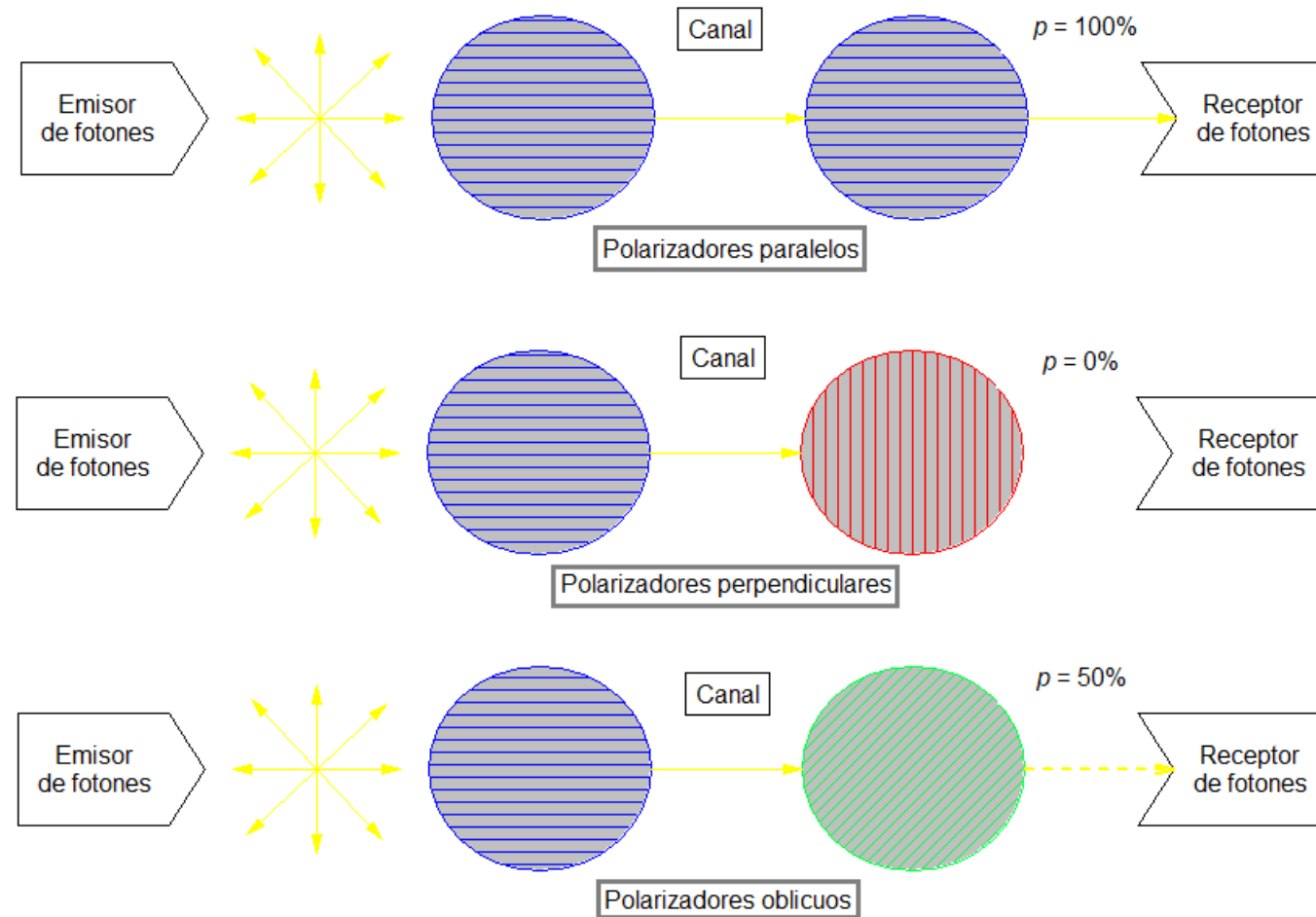
- Cuando una fuente de luz natural (el sol) o no coherente (una bombilla) emite fotones, cada fotón está polarizado en una polarización distinta, en todos los ángulos posibles.
- Cuando los fotones pasan a través de un filtro polarizador, su polarización queda fijada por el eje de transmisión del polarizador.
- Una vez fijada la polarización del fotón, si se coloca un segundo filtro, el fotón atravesará, o no, el segundo filtro dependiendo del ángulo que forme el segundo filtro respecto al primero. Esto es, los fotones continuarán su camino cambiando la polarización del fotón con una cierta probabilidad (Principio de incertidumbre).

Fotones polarizados



Filtros polarizadores

- Si los dos filtros son paralelos, el fotón siempre atravesará el polarizador (probabilidad = 1), pero si los filtros son perpendiculares, el fotón nunca atravesará el polarizador (probabilidad = 0).
- Entre los valores de 0° (filtros paralelos) y 90° (filtros perpendiculares) se pueden dar todos los ángulos posibles.
- Por tanto, la probabilidad de que el fotón pase los dos filtros variará entre 0 y 1.
- ❖ Si el ángulo de los dos filtros es de 45° , el fotón atravesará el segundo filtro con probabilidad = 0.5.



Protocolo de transmisión cuántica de claves de Bennett, B92, (1)

El **emisor** procede como sigue:

1. Genera una secuencia aleatoria de bits (mediante un generador de bits realmente aleatorio, TRBG) y la almacena de modo secreto (parte de esta secuencia será la clave que compartirá con el receptor).
2. Utiliza una base de polarización con filtros vertical, , y diagonal a 45°, , para codificar el envío del bit 0 o del bit 1, respectivamente.

El **receptor** conoce la base de polarización del emisor y su correspondiente codificación:  (0) y  (1) y el número de fotones a enviar. El receptor ejecuta los siguientes pasos:

1. Elige una base de polarización perpendicular a la del emisor con los filtros polarizados horizontal, , y diagonalmente a 135° (-45°), .
2. Genera aleatoriamente (mediante un TRBG) una secuencia de bits y codifica los filtros de modo que el horizontal, , codifica un bit 1 y el diagonal, , codifica un bit 0.

Protocolo de Bennett, B92, (2)

Una vez que el emisor comience a enviar fotones, el **receptor solo recibirá algunos de los fotones emitidos** por el emisor.

Si en una unidad de tiempo prefijada, el **receptor no recibe un fotón** es porque:

1. Su filtro estaba colocado perpendicularmente al considerado por el emisor, $\uparrow \leftrightarrow$ o $\nearrow \nwarrow$. Es decir, el bit del emisor es un 0 y el del receptor un 1, $\uparrow \leftrightarrow$, o el del emisor es un 1 y el del receptor un 0, $\nearrow \nwarrow$. Así, por la perpendicularidad de los filtros, el receptor no recibe ningún fotón.
2. Su filtro formaba con el del emisor un ángulo de 45° , $\uparrow \nwarrow$ o $\nearrow \leftrightarrow$, pero fue bloqueado por el segundo filtro (probabilidad = 0.5).

Por el contrario, si **el receptor recibe un fotón** se debe a que:

- Su filtro forma un ángulo de 45° con el del emisor y el fotón no fue bloqueado por el segundo filtro (probabilidad = 0.5).

Por tanto, si la polarización del receptor es diagonal, $\nwarrow$ (bit 0), se puede asegurar que el emisor empleaba un filtro polarizado verticalmente, $\uparrow$ (el bit era 0).

Si el filtro del receptor estuviera polarizado horizontalmente, $\leftrightarrow$ (bit 1), el filtro del emisor estaba polarizado diagonalmente, $\nearrow$ (bit 1).

Protocolo de Bennett, B92, (3)

- Cuando el receptor recibe un fotón señala el hecho como “acierto” y anota el bit de su secuencia que corresponde a la polarización que emplea en ese momento.
- Transmitidos todos los fotones, el receptor comunica al emisor, por un **canal autenticado**, las posiciones de su lista de bits que son sus “aciertos”, pero no las polarizaciones.
- Al final, el emisor y el receptor usarán como clave compartida los bits de tales posiciones.

Bits del emisor	0	1	0		1	
Polarización del emisor	↕	↗	↕		↗	
Bits del receptor	1	0	0		1	
Polarización del receptor	↔	↖	↖		↔	
Llega fotón al receptor	No	No	No	Sí	No	Sí
Bit de la clave compartida	-	-		0		1

Al receptor le llega un fotón con probabilidad = 0.25 (la mitad son 0 y la otra mitad 1)

3. Computación cuántica

Google: supremacía cuántica

EL PAÍS

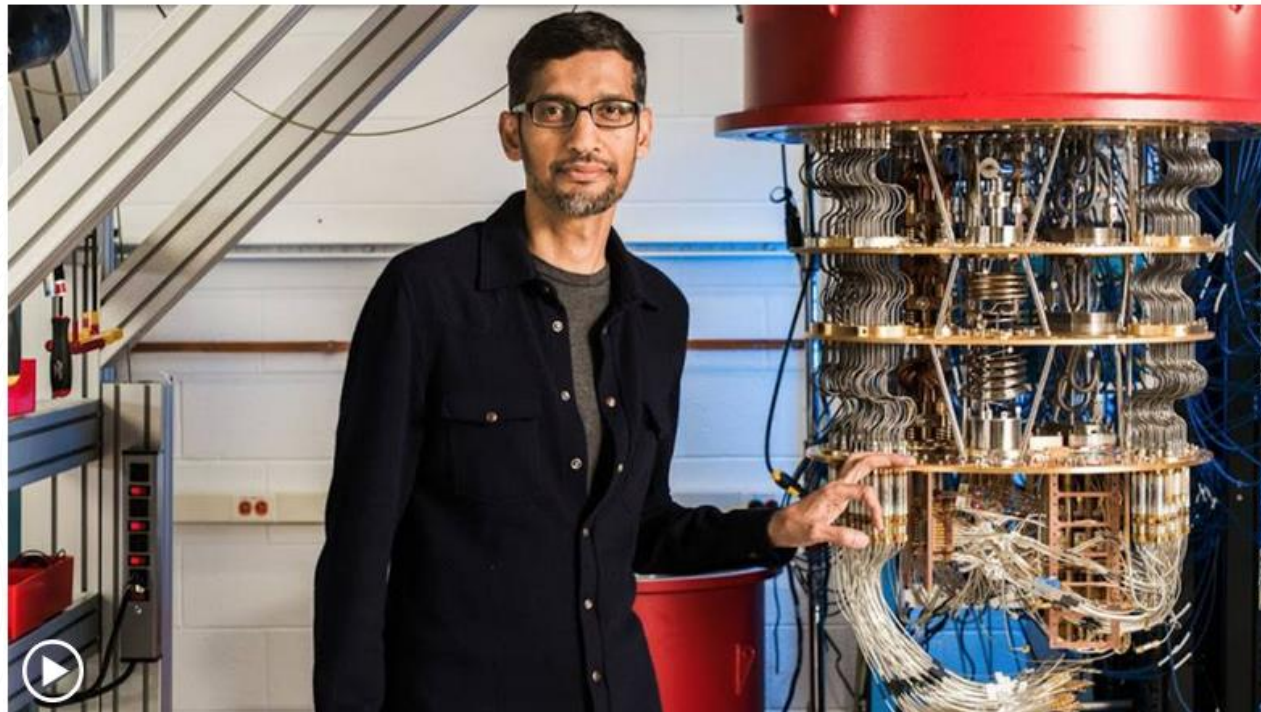
TECNOLOGÍA

SUSCRÍBETE



Google explica por fin cómo ha logrado la supremacía cuántica

La compañía publica en la revista 'Nature' el mayor avance de la historia en computación cuántica, aunque IBM niega que el experimento de la empresa de Silicon Valley dé el resultado que presenta

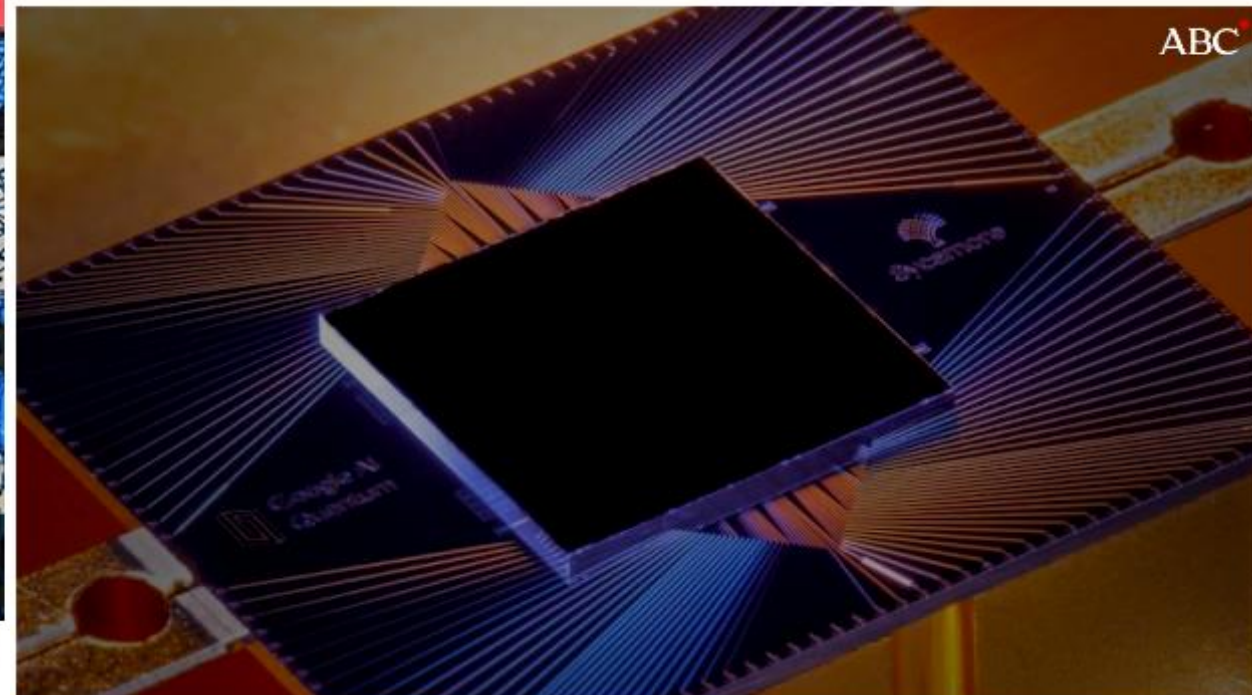


Sundar Pichai, presidente ejecutivo de Google, junto a uno de los ordenadores cuánticos de la compañía en su laboratorio de Santa Barbara (California). En vídeo, Pichai explica el presunto mayor avance en la historia de la computación cuántica. GOOGLE

ABC CIENCIA

Google publica la demostración de la supremacía cuántica

- La compañía explica en «Nature» cómo su ordenador cuántico ha realizado un cálculo más allá del alcance del procesador clásico más avanzado del mundo
- Tardó 200 segundos en ejecutar una tarea que a la máquina más rápida le habría llevado 10.000 años
- IBM ya rechazó el lunes que el hito se haya conseguido



ABC

IBM: ventaja cuántica

- Google publicó en Nature que había logrado la **supremacía cuántica** con su ordenador de 53 *qubits* al resolver un problema de generación de números aleatorios en 3'20", que a un ordenador convencional le costaría 10.000 años.
- IBM contestó que un superordenador podría hacerlo en dos días y medio (con mayor fidelidad) y que Google solo ha logrado una **ventaja cuántica**.
- ✓ Google eligió una tarea muy específica (y con poca relevancia práctica) que a un ordenador cuántico se le daría muy bien pero que a uno convencional le costaría mucho.
- ✓ Simular un ordenador cuántico en uno convencional requiere almacenar grandes cantidades de datos. A menor memoria, más pasos en la tarea a realizar y más tiempo.
- ✓ IBM propuso usar tanto memoria como disco duro.

Article

Quantum supremacy using a programmable superconducting processor

<https://doi.org/10.1038/s41586-019-1666-5>

Received: 22 July 2019

Accepted: 20 September 2019

Published online: 23 October 2019

Frank Arute¹, Kunal Arya¹, Ryan Babbush¹, Dave Bacon¹, Joseph C. Bardin^{1,2}, Rami Barends¹, Rupak Biswas³, Sergio Boixo¹, Fernando G. S. L. Brandao^{4,5}, David A. Buell¹, Brian Burkett¹, Yu Chen¹, Zijun Chen¹, Ben Chiaro⁶, Roberto Collins¹, William Courtney¹, Andrew Dunsworth¹, Edward Farhi¹, Brooks Foxen^{1,5}, Austin Fowler¹, Craig Gidney¹, Marissa Giustina¹, Rob Graff¹, Keith Guerin¹, Steve Habegger¹, Matthew P. Harrigan¹, Michael J. Hartmann^{1,6}, Alan Ho¹, Markus Hoffmann¹, Trent Huang¹, Travis S. Humble⁷, Sergel V. Isakov¹, Evan Jeffrey¹, Zhang Jang¹, Dvir Kafri¹, Kostyantyn Kechedzhil¹, Julian Kelly¹, Paul V. Klimov¹, Sergey Knysch¹, Alexander Korotkov^{1,8}, Fedor Kostritsa¹, David Landhuis¹, Mike Lindmark¹, Erik Lucero¹, Dmitry Lyakh⁹, Salvatore Mandrà^{3,10}, Jarrod R. McClean¹, Matthew McEwen⁵, Anthony Megrant¹, Xiao Mi¹, Kristel Michielsen^{1,12}, Masoud Mohseni¹, Josh Mutus¹, Ofer Naaman¹, Matthew Neeley¹, Charles Neill¹, Murphy Yuezhen Niu¹, Eric Ostby¹, Andre Petukhov¹, John C. Platt¹, Chris Quintana¹, Eleanor G. Rieffel³, Pedram Roushan¹, Nicholas C. Rubin¹, Daniel Sank¹, Kevin J. Satzinger¹, Vadim Smelyanskiy¹, Kevin J. Sung^{1,13}, Matthew D. Trevithick¹, Amit Vainsencher¹, Benjamin Villalonga^{1,14}, Theodore White¹, Z. Jamie Yao¹, Ping Yeh¹, Adam Zalcman¹, Hartmut Neven¹ & John M. Martinis^{1,5*}

The promise of quantum computers is that certain computational tasks might be executed exponentially faster on a quantum processor than on a classical processor¹. A fundamental challenge is to build a high-fidelity processor capable of running quantum algorithms in an exponentially large computational space. Here we report the use of a processor with programmable superconducting qubits^{2–7} to create quantum states on 53 qubits, corresponding to a computational state-space of dimension 2^{53} (about 10^{16}). Measurements from repeated experiments sample the resulting probability distribution, which we verify using classical simulations. Our Sycamore processor takes about 200 seconds to sample one instance of a quantum circuit a million times—our benchmarks currently indicate that the equivalent task for a state-of-the-art classical supercomputer would take approximately 10,000 years. This dramatic increase in speed compared to all known classical algorithms is an experimental realization of quantum supremacy^{8–14} for this specific computational task, heralding a much-anticipated computing paradigm.

¿Es mi ordenador es mejor que el tuyo?

La respuesta, en la **computación clásica**, depende de varios factores:

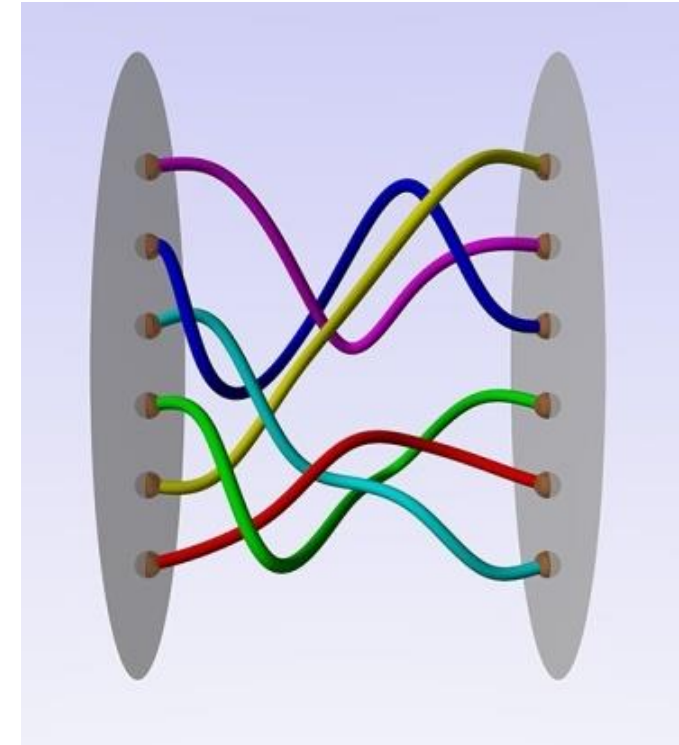
- Cantidad de memoria, Tipo y capacidad de disco duro, Procesador, Número de núcleos, Tarjeta gráfica, Tipos y número de conectores, etc.
- Pero sobre todo, la respuesta depende de si es capaz de resolver **MIS** problemas.

De forma análoga, en **computación cuántica**, no basta con tener más *qubits*.

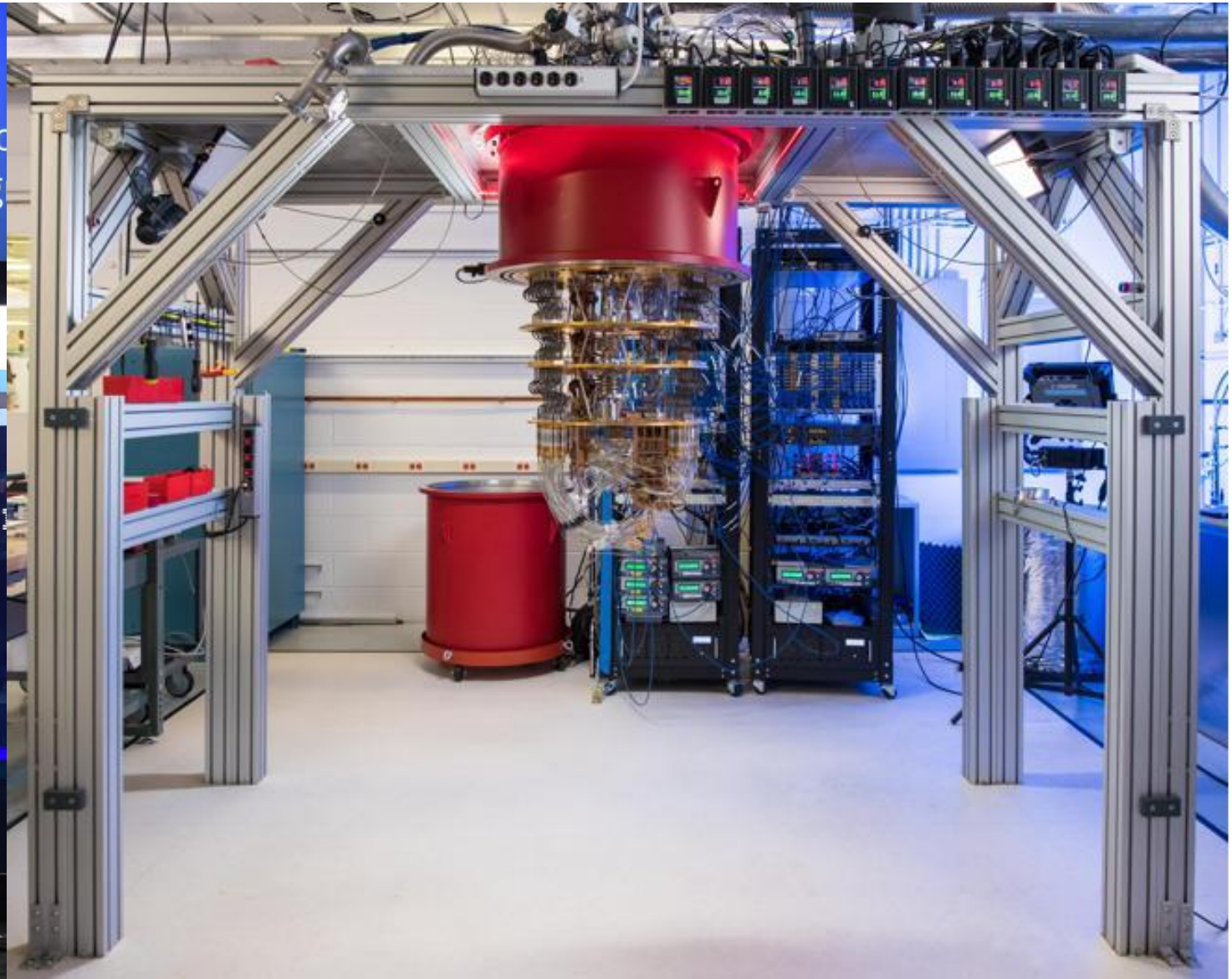
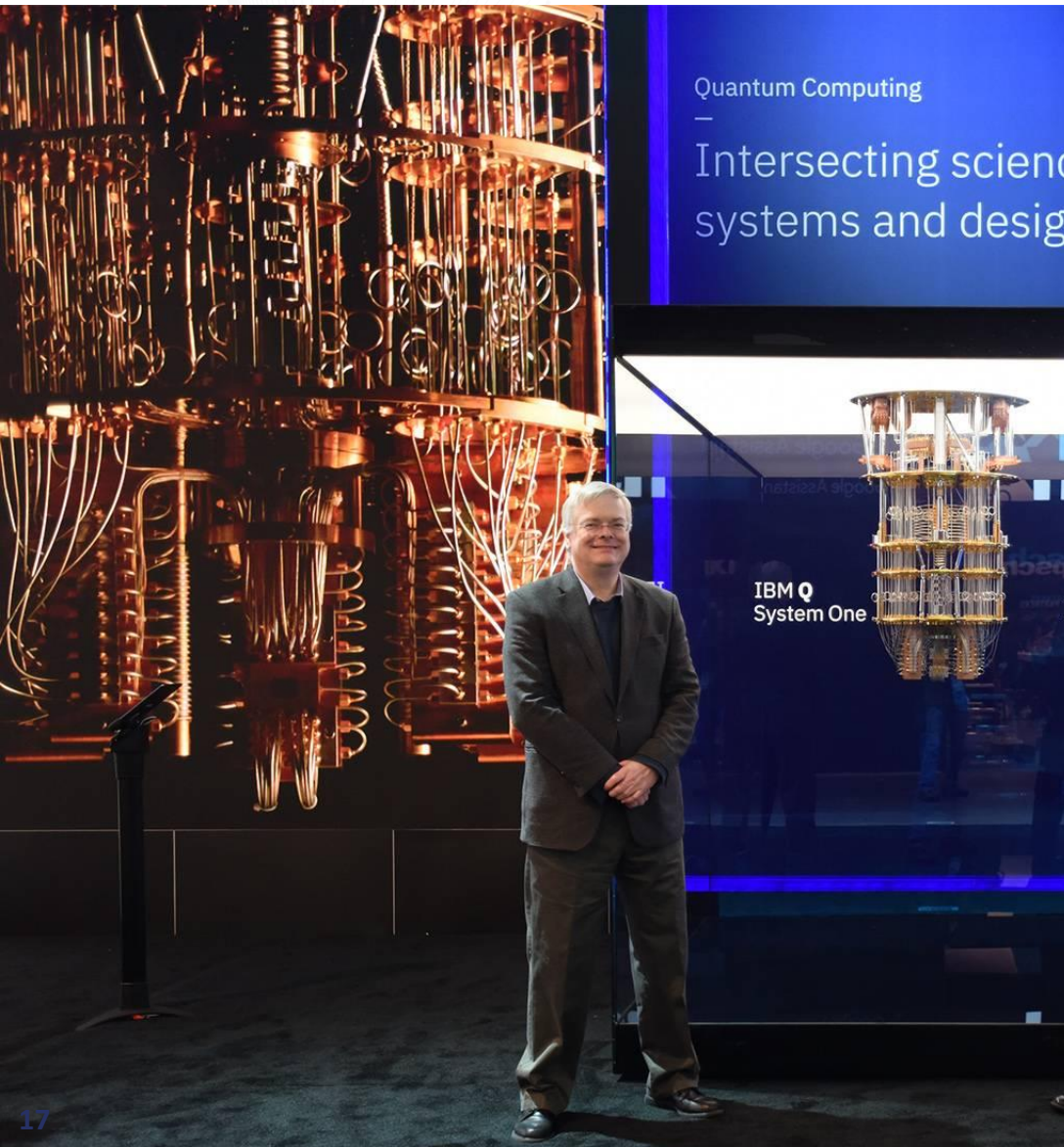
- El problema no es sobre la cantidad de *qubits* sino sobre su calidad, esto es, *qubits* con baja tasa de error y circuitos con conectividad duradera.
- IBM ha propuesto que la **potencia de un ordenador cuántico** se exprese a través de la métrica “**volumen cuántico**”, que incluye el número de *qubits*, la calidad de las operaciones cuánticas, la conectividad del *qubit* y el paralelismo cuántico.

Computador cuántico topológico de Microsoft

- Microsoft considera que un ***qubit topológico*** estará menos afectado por los cambios en su entorno (mayor estabilidad y resistencia al ruido ambiental), lo que facilitará la corrección de errores y serán más confiables durante más tiempo.
- El sistema se basa en unas cuasipartículas llamadas *anyons* no abelianas. La información no se codifica en las cuasipartículas, sino en el orden en que se intercambian las posiciones de los *anyons* (**trenzado**).
- La información está codificada en una **propiedad topológica** de los *anyons*, que es una propiedad colectiva del sistema y que solo cambia con movimientos macroscópicos.



Computador cuántico universal de IBM/Google



Computador cuántico D-Wave

- Los sistemas de computación cuántica (basados en el principio de superposición) para buscar soluciones óptimas.
- Abordan problemas de optimización combinatoria)
- ❖ Los sistemas de computación cuántica (basados en el principio de superposición) abajo, las cosas se complican. En un mundo cuántico, la bola rodará a un mínimo global que soltará mucho ruido.
- Los sistemas de computación cuántica (basados en el principio de superposición) a la vez (superposición) los mínimos locales.
- Capacidad actual de 20000 qubits.
- Los sistemas de computación cuántica (basados en el principio de superposición) son universales).



quantum annealing)
das.

de optimización

etos caen cuesta
e la colina, la bola
ínimo global hay

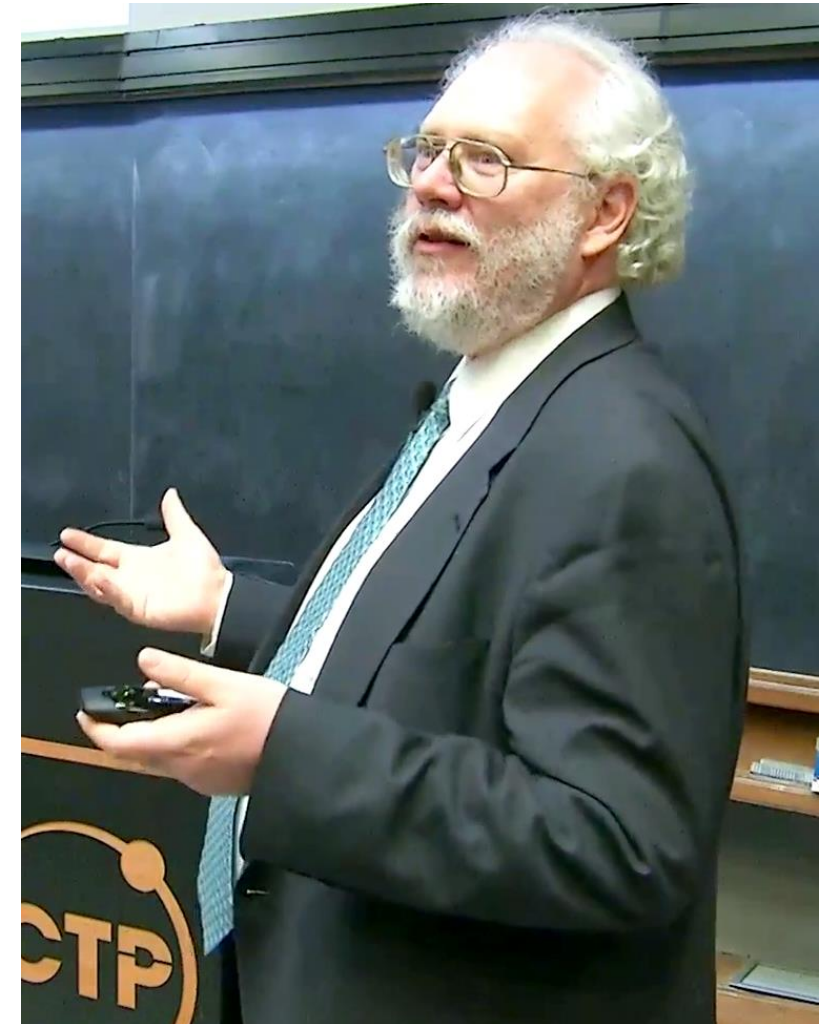
a muchas posiciones
abilidad de alcanzar

son universales).

4. Criptoanálisis cuánticos

Algoritmo de Shor

- En 1997 (1994/95), Shor publicó un artículo proponiendo dos algoritmos que pueden **romper el problema de la factorización de enteros (RSA) y el del logaritmo discreto (ECC)** utilizados en la criptografía asimétrica moderna, en tiempo polinómico, **si existiera un ordenador cuántico.**



PROBLEMAS MATEMÁTICOS

Problemas matemáticos y
computación cuántica

Problemas
difícilmente
computables
(tiempo
exponencial)

-logaritmo discreto

Problemas fácilmente
computables
(tiempo polinómico)

Problemas
cuánticamente
resolubles

-factorización

Aplicaciones
cuánticas

Algoritmo de Grover

- Grover publico (1997) un algoritmo por el que la computación cuántica reduciría el tiempo necesario para **romper la criptografía simétrica** a la raíz cuadrada del tiempo actual.
- Un ordenador cuántico tardara el mismo tiempo en realizar una búsqueda exhaustiva de claves de 256 bits que un PC actual en un espacio de claves de 128 bits.

No obstante, resultados recientes apuntan a que la criptografía simétrica podría no resistir la computación cuántica, dado que se han encontrado **aceleraciones exponenciales en ataques a sistemas criptográficos simétricos** (paralelización del algoritmo de Simon).



La criptografía actual tiene los días contados

- Todos los criptosistemas y protocolos basados en el **Problema de la Factorización de Enteros** (IFP) o en el **Problema del Logaritmo Discreto** (DLP) son vulnerables a la computación cuántica (RSA, ElGamal, ECC, DH, ECDH, Firma RSA, DSA, ECDSA, HTTPS, TLS, PGP, GPG, etc.).
- Los **criptosistemas simétricos** (TDES, AES, Blowfish, etc.) verían amenazada su seguridad por la **reducción de las longitudes de sus claves a la mitad**. Pero podría ser peor si las investigaciones sobre la paralelización del algoritmo de Simon acabaran demostrando que son vulnerables.
- La pregunta a la que nadie tiene respuesta es: **¿cuál será la fecha de caducidad?**
- Un botón: Romper un RSA-2048 en 8 horas con 20 millones de noisy *qubits* (Gidney & Ekerä).

5. El futuro se llama criptografía postcuántica

Llamada del NIST

- En noviembre de 2017 se aceptaron 69 algoritmos en la Ronda 1 y muy pronto se retiraron 5 después de numerosos comentarios.
 - <https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions>
- En enero de 2019 se ha publicado la lista de los algoritmos que se mantienen en la Ronda 2.
 - <https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions>
- 22-24 Agosto 2019: Second PQC Standardization Conference

Fechas futuras:

- 2020/2021: Inicio de la Ronda 3 o algoritmos seleccionados
- 2022/2024: Publicación del primer Draft Standards

Ronda 2: Criptosistemas y Protocolos de acuerdos de clave

CÓDIGOS CORRECTORES DE ERRORES

CIFRADOS ASIMÉTRICOS

- **HQC**: Códigos cuasícíclicos y códigos BCH.
- **LEDAcrypt** suite: Códigos cuasícíclicos de baja densidad.
- **ROLLO** (Rank-Ouroboros, LAKE and LOCKER).
- **RQC**: Códigos ideales y códigos de Gabidulin.

MECANISMOS DE ENCAPSULACIÓN DE CLAVES (KEM)

- **BIKE** suite: Códigos cuasícíclicos de densidad moderada.
- **Classic McEliece**.
- **NTS-KEM**.

PROBLEMAS DEFINIDOS EN RETÍCULOS

CIFRADOS ASIMÉTRICOS

- **NTRU Prime** family: Anillos sin estructuras.
- **Round5**: Aprendizaje general con redondeo (GLWR).
- **SABER**: Aprendizaje con errores en módulos (MLWR).

MECANISMOS DE ENCAPSULACIÓN DE CLAVES (KEM)

- **NewHope**: Aprendizaje con errores en anillos (Ring-LWE).
- **CRYSTALS-KYBER** (Cryptographic Suite for Algebraic Lattices).
- **FrodoKEM** family: Aprendizaje con errores (LWE).

ISOGENIAS DE CURVAS ELÍPTICAS – KEM

- **SIKE**: Recorridos pseudoaleatorios.

Ronda 2: Algoritmos de firma digital

PROBLEMAS DEFINIDOS EN RETÍCULOS

- **CRYSTALS-DILITHIUM** (Cryptographic Suite for Algebraic Lattices).
- **Falcon**: Propuesta de Gentry, Peikert y Vaikuntanathan para esquemas de firma basados en retículos.
- **qTESLA**: Aprendizaje con errores en anillos (decisional).

PROBLEMA MULTIVARIANTE CUADRÁTICO

- **GeMSS** (Great Multivariate Short Signature): Ecuaciones de cuerpo oculto (HFE) utilizando los modificadores de vinagre menos (HFEv-).
- **LUOV** = UOV (Unbalanced Oil and Vinegar) + PRNG + Field Lifting + Simplified Secret Key.
- **MQDSS**: Paradigma de Fiat-Shamir de transformación de esquemas de identificación segura.

FUNCIONES HASH

- **SPHINCS⁺**.

Referencias

- ❑ F. Arute et al., *Quantum supremacy using a programmable superconducting processor*, Nature, 574, 505-511, 23/10/2019.
- ❑ C. Bennett, *Quantum cryptography using any two nonorthogonal states*, Phys. Rev. Lett. 68 (1992), 3121-3124.
- ❑ D.J. Bernstein, J. Buchmann, and E. Dahmen (Eds.), *Post-Quantum Cryptography*, Springer, Heidelberg, 2009.
- ❑ A. Bocharov, *Inside Microsoft's quest for a topological quantum computer*, Nature, doi:10.1038/nature.2016.20774
- ❑ C. Gidney & M. Eker, *How to factor 2048 bit RSA integers in 8 hours using 20 millions noisy qubits*, arXiv: 1905.09749v1, 23/5/2019.
- ❑ K.L. Grover, *Quantum mechanics helps in searching for a needle in a haystack*, Phys. Rev. Lett. 79 (1997), 325-328.
- ❑ M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia, *Quantum differential and linear cryptanalysis*, IACR Trans. Symmetric Cryptol. 1(2016), 71-94.
- ❑ P.W. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM J. Computing 5, 26 (1997), 1484-1509.

COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

**XIII
JORNADAS
STIC
CCN-CERT**

ccn-cert
centro criptológico nacional