La Amenaza Cuántica a la Ciberseguridad: Desafíos y Soluciones

Jordi Prieto Gallego

Hack0n – 22/02/2024

¿QUIÉNES SOMOS?

Sobre mí

Jordi Prieto Gallego

jtsec Beyond IT Security

jprieto@jtsec.es

- Background en Física y Matemáticas (UGR)
- Especialista Criptográfico y Analista de Entropía
- Experto en metodologías de evaluación FIPS 140-3, MEMeC, AIS-20/31 y SP 800-90B
- Análisis de soluciones post-cuánticas
- Miembro de CMUF
- Certificate of Quantum Excellence, IBM

Sobre nosotros

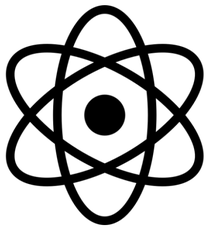
- Servicios de evaluación y consultoría en ciberseguridad, con equipo de Criptografía
- Laboratorio acreditado Common Criteria, LINCE y ETSI EN 303 645
- Desarrolladores de la herramienta más avanzada para Common Criteria, CCToolbox
- Implicados en actividades de estandarización (ISO, CEN/CENELEC, ISCI WGs, ENISA CSA WGs, CCUF, CMUF, ERNCIP, …)
- Miembros del SCCG (Stakeholder Cybersecurity Certification Group)
- jtsec forma parte del grupo Applus+ junto con Lightship Security. Disponemos de laboratorios en Canadá, EEUU y España

ÍNDICE

MECÁNICA CUÁNTICA DEL QUBIT

MECÁNICA CUÁNTICA

- Teoría desarrollada desde los años 20
- Una de las teorías físicas más precisas y contrastadas
- Antiintuitiva para los Homo Sapiens: entrelazamiento, superposición, colapso del estado cuántico…



- Es una teoría probabilística
- A partir de pocos axiomas permite calcular la probabilidad de los resultados de las medidas

- La mecánica cuántica describe, evoluciona y mide estados cuánticos de sistemas
- Un estado cuántico contiene toda la información que se puede saber sobre un sistema cuántico
- Representados por vectores en espacios vectoriales complejos

$$|\psi\rangle$$

BITS Y QUBITS

Definición

- **Bit:** unidad básica de información clásica. Representado por dos valores enteros, 0 y 1
- **Qubit:** unidad básica de información cuántica y sistema cuántico más simple. Se representa como una combinación lineal de los vectores 0 y 1 de la base computacional
- **Muchísimos (!!!) más estados posibles**

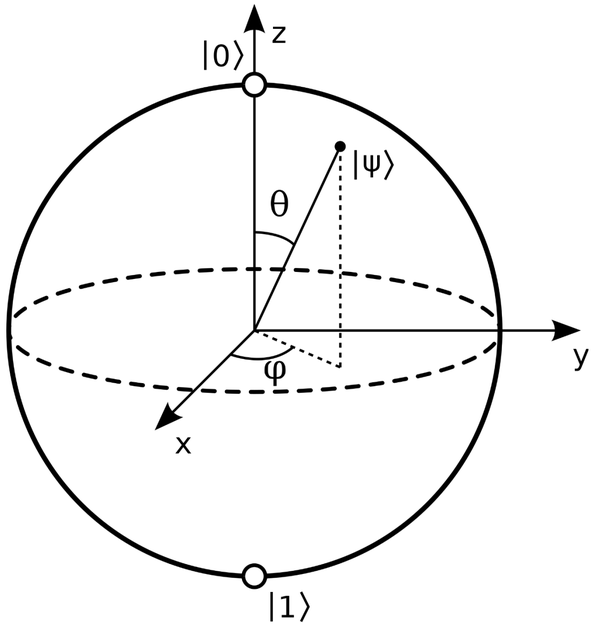
$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle =$$

$$\alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} =$$

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

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

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

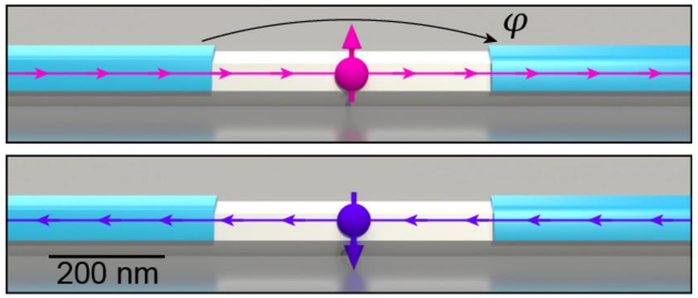


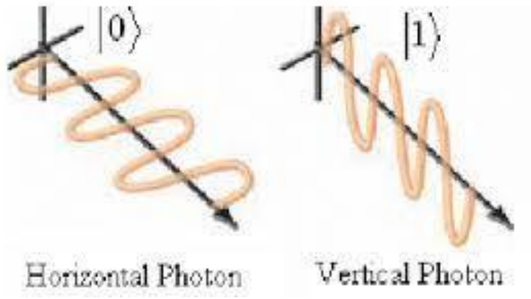
BITS Y QUBITS

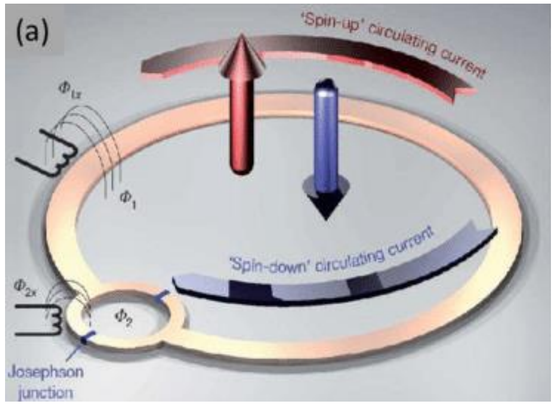
Implementaciones Físicas

- **Bit:** transistores
- **Qubit:** sistemas cuánticos de dos estados. Iones atrapados de los que se pueda medir su espín, polarización de fotones, circuitos superconductores

Los qubits son mucho más frágiles → decoherencia cuántica







BITS Y QUBITS

Evolución

- **Bit:** sólo podemos aplicar NOT, transformando 0 en 1 y viceversa
- **Qubit:** aplicando puertas lógicas cuánticas a un qubit, lo podemos evolucionar a cualquier otro.

La evolución de un qubit es determinista, matemáticamente se trata de álgebra lineal

$$|\psi'\rangle = U|\psi\rangle = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

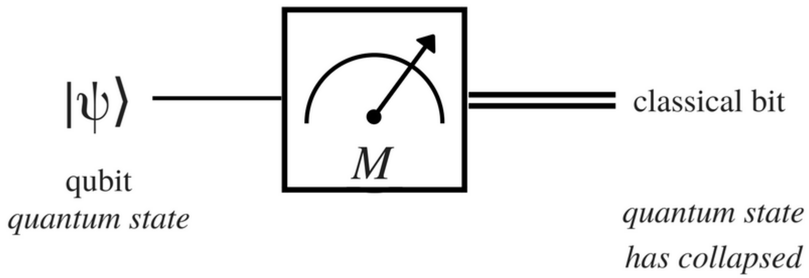
BITS Y QUBITS

Medición

- **Bit:** al medirlo se obtiene directamente su estado, sin alterar la información. **Es un proceso determinista**
- **Qubit:** Al realizar una medida, el estado de superposición del qubit "colapsa" a uno de los estados base (0 o 1). **Es un proceso probabilístico**

El proceso de medida supone pasar del “mundo cuántico” al mundo “clásico”

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \rightarrow \begin{cases} |0\rangle & \text{con probabilidad } |\alpha|^2, \\ |1\rangle & \text{con probabilidad } |\beta|^2. \end{cases}$$



COMPUTANDO CON QUBITS

Jugando con más qubits

- Podemos pasar de un qubit a un sistema de 2, 3…
- Un sistema de N qubits se representa mediante un vector complejo de 2^N dimensiones complejas. Esto se va de las manos muy rápido; los estados de varios qubits son “muy grandes”

Ejemplo: si representamos cada complejo con dos flotantes de 8 bytes y le damos una capacidad computacional de 1PB a cada humano, sólo tendríamos para 78 qubits

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle = \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix}, \quad \text{donde } \alpha, \beta, \gamma, \delta \in \mathbb{C}$$

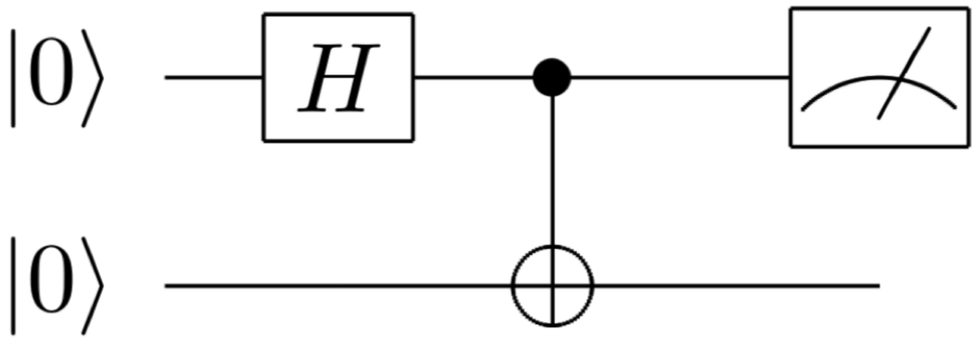
$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$$

COMPUTANDO CON QUBITS

Circuito cuántico

- **Preparación:** Los qubits se inicializan en un estado conocido, típicamente |0⟩, preparando el sistema para la computación cuántica
- **Evolución:** Una secuencia de puertas cuánticas (operaciones unitarias) se aplica a los qubits para manipular sus estados. Estas puertas pueden cambiar estados individuales, entrelazar qubits, y más…
- **Medición:** al final del circuito, los qubits se miden, colapsando su estado cuántico a un estado clásico (0 o 1). El resultado de estas mediciones se utiliza para obtener la salida del cálculo cuántico

La capacidad de cómputo aumenta exponencialmente con el número de qubits



COMPUTANDO CON QUBITS

Algoritmos cuánticos: el mito

- Muchos creen que un algoritmo cuántico realiza todas las soluciones posibles en paralelo, aprovechando el "poder mágico" de la computación cuántica para resolver problemas instantáneamente.

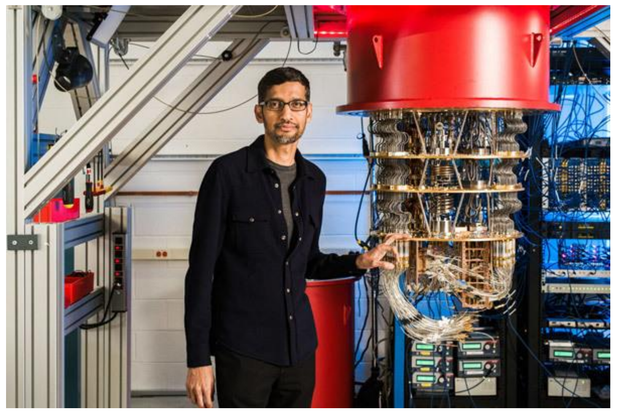
Algoritmos cuánticos: la realidad

- Utilizan la coordinación de interferencias cuánticas a través de puertas lógicas cuánticas, aprovechando las propiedades de superposición y entrelazamiento de los qubits. Esto permite manipular el estado cuántico de manera que, **al medir, se pueda maximizar la probabilidad de obtener la solución correcta al problema**
- De forma muy astuta, **para algunos problemas se han encontrado algoritmos cuánticos mucho más eficientes** que los algoritmos clásicos conocidos
- Su uso más evidente es la **simulación de sistemas cuánticos**: esto traerá una revolución en ciencia de materiales, farmacología, química orgánica…

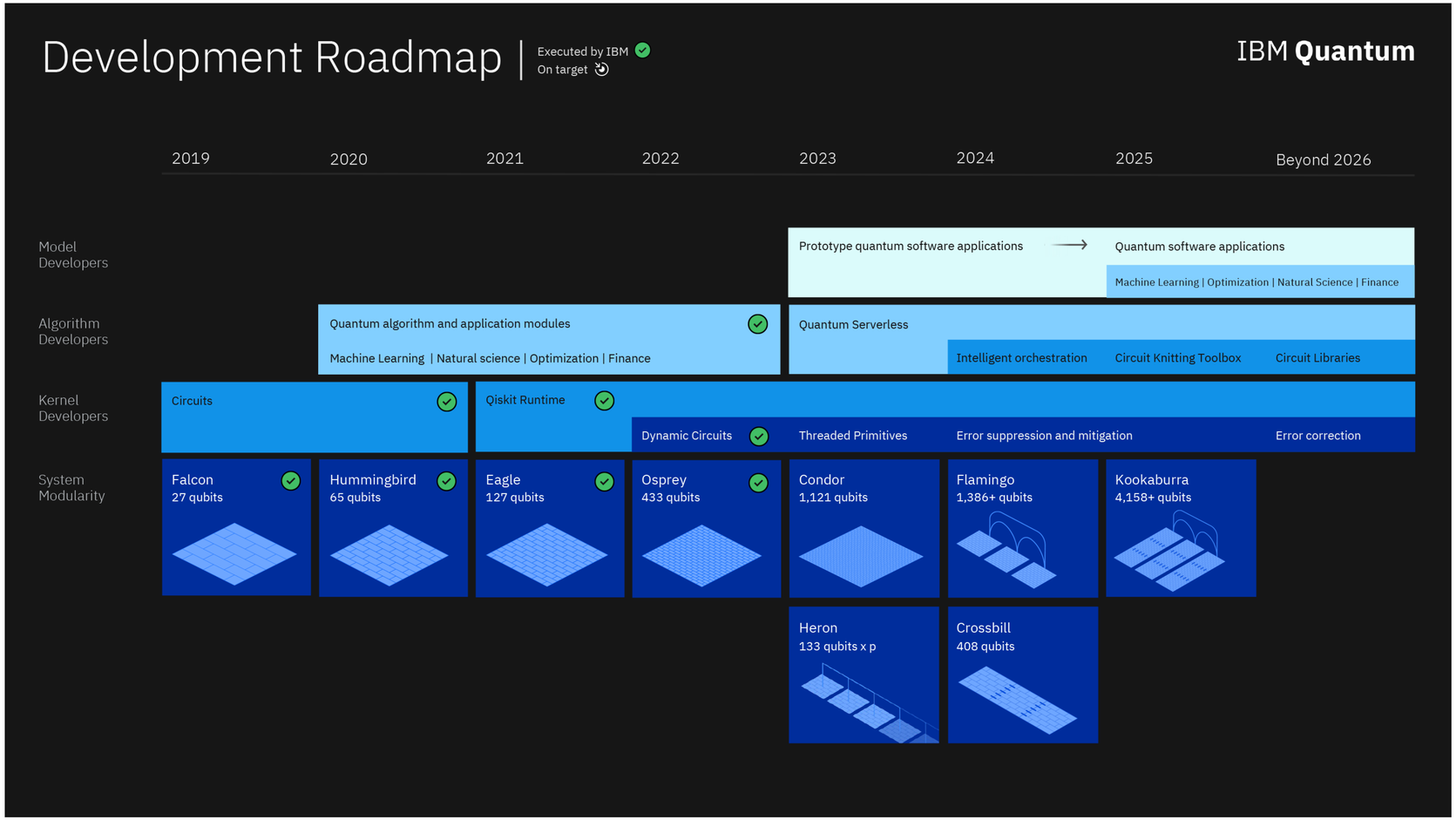
ORDENADORES CUÁNTICOS ACTUALES

Noise Intermediate Quantum Computers

- Actualmente tienen el orden de los 100 qubits físicos (Osprey IBM, con 433)
- Afectados por el ruido cuántico (decoherencia) y no aplican corrección de errores completa
- **Reto intelectual:** mejorar la corrección de errores cuántica → se requieren muchos qubits físicos para obtener uno lógico (Teorema de No-Clonado)
- **Reto de ingeniería:** mantener estados cuánticos, mejorar tasas de error, topología de los qubits, aumentar el número de qubits lógicos
- **Supremacía Cuántica (2019)** → 200 segundos con 52 qubits vs 10000 años con supercomputador



ORDENADORES CUÁNTICOS ACTUALES



ÍNDICE

CRIPTOGRAFÍA MODERNA

Seguridad

- = suposición de que ciertos problemas matemáticos, en los que se basa, son demasiado complejos para ser resueltos eficientemente
- No existen demostraciones matemáticas que demuestren que dicha dificultad es insuperable
- La complejidad computacional de un problema es la del algoritmo conocido capaz de resolverlo de forma más eficiente

Ejemplos

- RSA → factorización de enteros
- FFC y ECC (DH, ECDH, ECDSA…) → logaritmo discreto

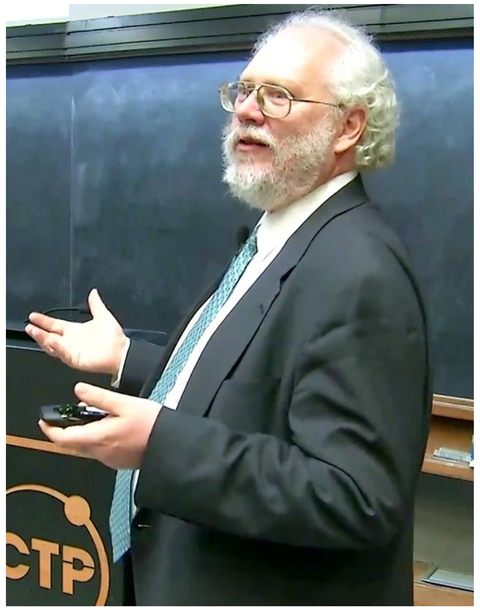
$$\text{Dada } N = pq, \text{ encontrar } p \text{ y } q,$$

$$\text{Dados } g \text{ y } h \text{ en un grupo finito, encontrar } x \text{ tal que } g^x = h.$$

CRIPTOGRAFÍA ASIMÉTRICA

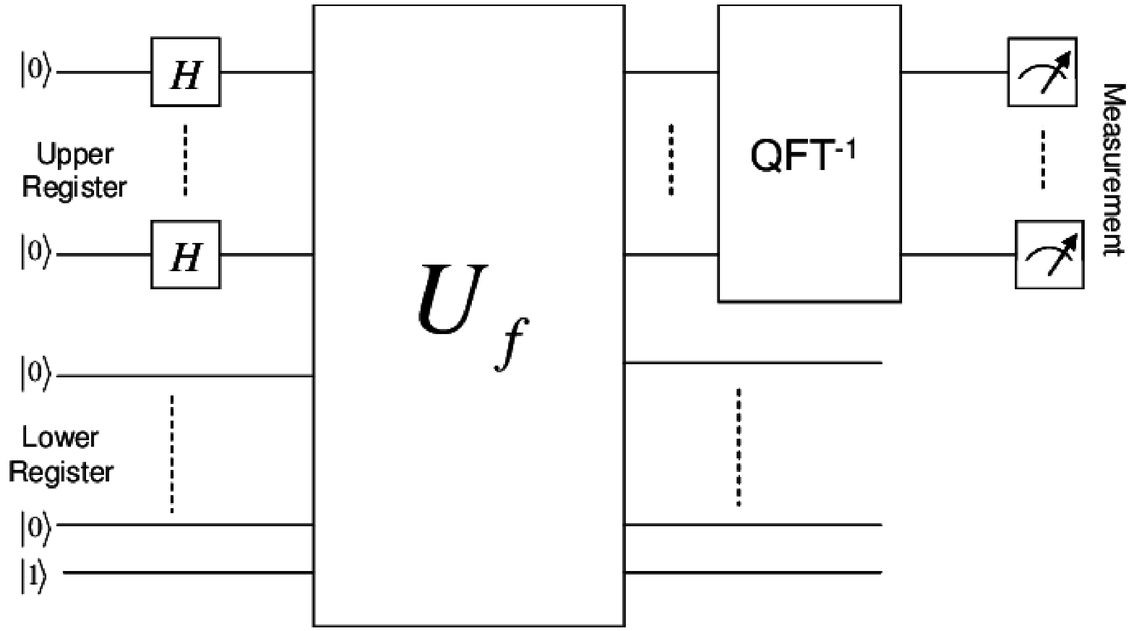
Algoritmo de Shor

- Shor, 1994. El gran impulso de la CQ
- Speed-up casi exponencial en la complejidad → **F en el chat para toda la criptografía asimétrica actual**
- Se espera que se requieran miles de qubits **lógicos**



1. Elegir un número aleatorio $a < n$.
2. Calcular el MCD de n y a usando el algoritmo de Euclides.
3. Si $\text{MCD}(a, n) \neq 1$, entonces se ha encontrado un factor no trivial de n.
4. Definir $f(x) = a^x \mod n$ y usar la transformada cuántica de Fourier para encontrar el período r de f.
5. Si r es impar o $a^{r/2} \equiv -1 (\mod n)$, volver al paso 1.
6. Los factores de n se pueden encontrar calculando $\text{MCD}(a^{r/2} \pm 1, n)$.

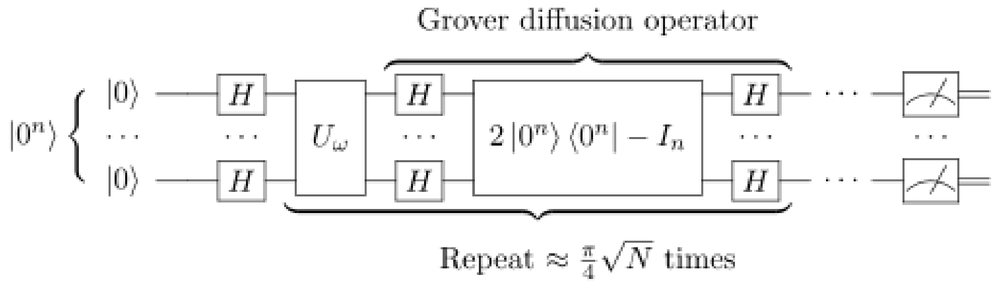
CRIPTOGRAFÍA ASIMÉTRICA



CRIPTOGRAFÍA SIMÉTRICA

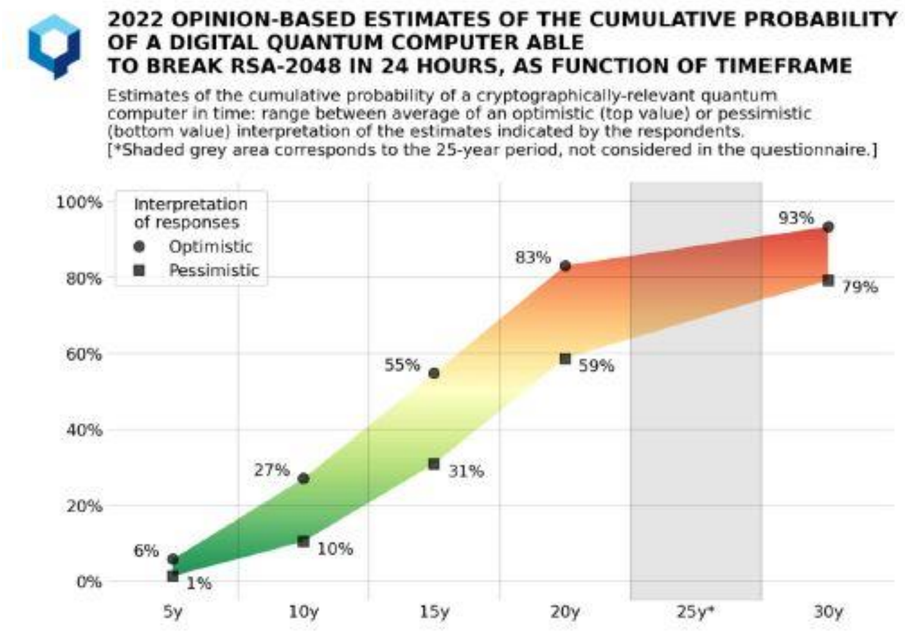
Algoritmos de Grover y Simon

- Speed-up cuadrático en la complejidad → **la solución es doblar el tamaño de las claves**
- Grover → Algoritmo de búsqueda

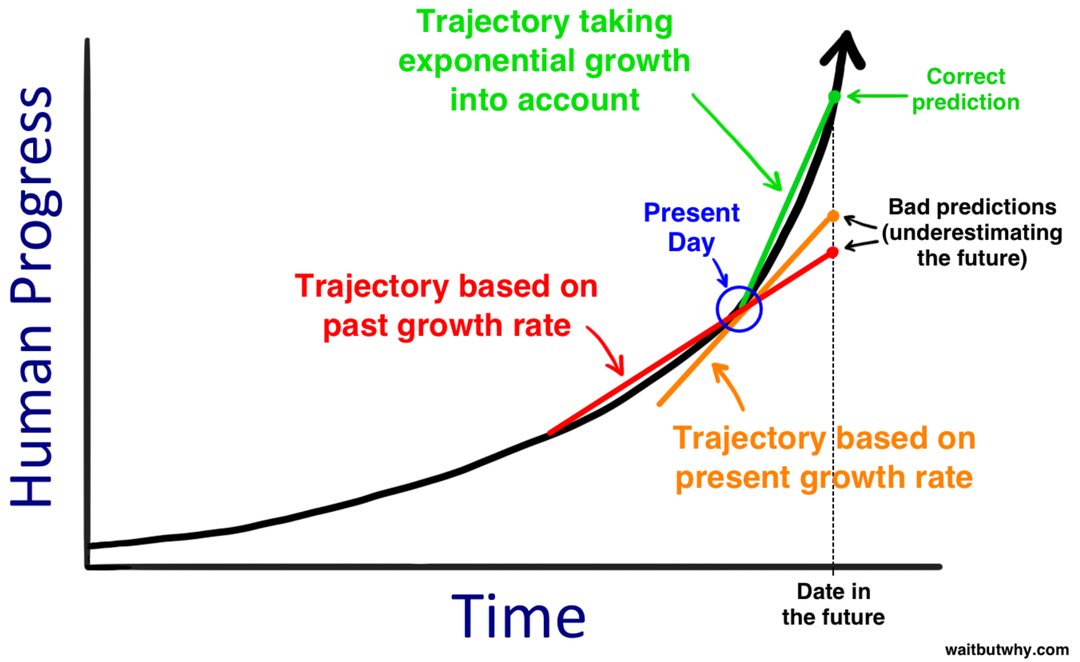


COMPUTACIÓN CUÁNTICA VS CRIPTOGRAFÍA

HUSTON, TENDREMOS UN PROBLEMA



Yes



But...

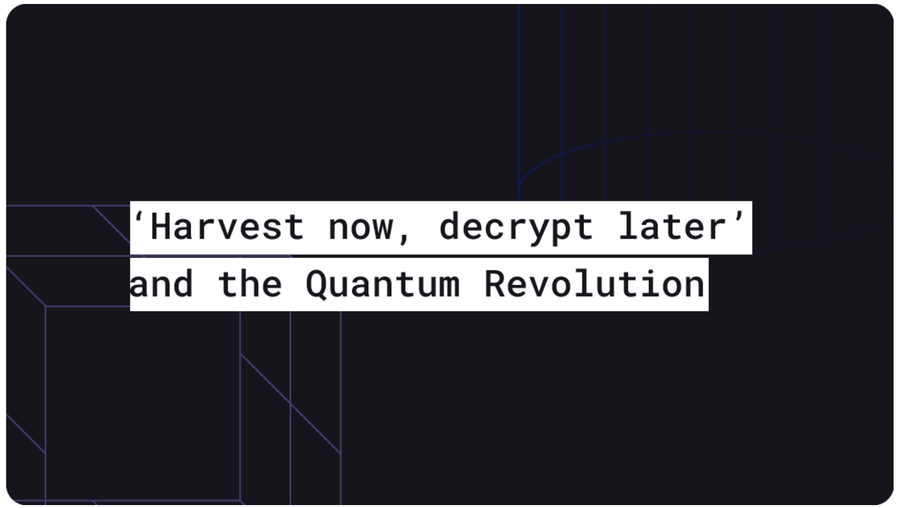
HUSTON, TENEMOS UN PROBLEMA

TEOREMA DE MOSCA

- Si x + y > z , tenemos un problema.

- X tiempo que deseamos que nuestros datos estén seguros.
- Y tiempo que llevará migrar nuestros sistemas a QR.
- Z tiempo que tardaran los ordenadores cuánticos en vulnerar nuestros sistemas.

Yes



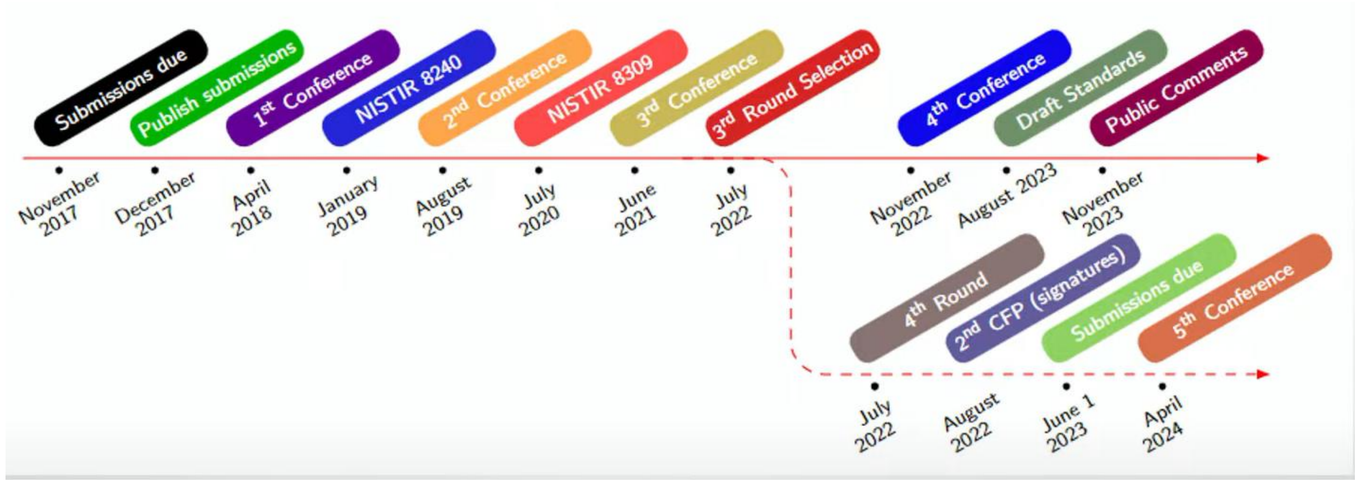
But…

ÍNDICE

UNA SOLUCIÓN…

Criptografía Post-Cuántica

- **La criptografía asimétrica actual es vulnerable → Criptografía asimétrica post-cuántica**
- Hace uso de algoritmos clásicos basados en problemas matemáticos para los que no se conocen algoritmos clásicos ni cuánticos eficientes que los resuelvan
- NIST ha lanzado un proceso de estandarización



PQC NIST

Criptosistema asimétrico y KEM	Área y problema matemático
CRYSTALS-Kyber	Retículo estructurado (MLWE)

Tabla 1. Candidato KEM seleccionado por el NIST después de la tercera ronda y primitiva matemática asociada

Firma digital	Área y problema matemático
CRYSTALS-Dilithium	Retículo estructurado (MLWE)
Falcon	Retículo estructurado (SIS)
SPHINCS$^+$	Funciones hash

Tabla 2. Candidatos a firma seleccionados por el NIST después de la tercera ronda y primitivas matemáticas asociadas

PQC NIST

Criptosistema asimétrico y KEM	Primitiva matemática
BIKE	Códigos de densidad moderada cuasi-cíclicos
HQC	Códigos cuasi-cíclicos de Hamming
Classic McEliece	Códigos de Goppa
SIKE†	Isogenias sobre curvas elípticas
†las últimas investigaciones han mostrado que el algoritmo SIKE es vulnerable, véase el párrafo 26	

Tabla 3. Candidatos a KEM para ser analizados por el NIST en la cuarta ronda y primitivas matemáticas asociadas

Wouter Castryck and Thomas Decru, research experts at the KU Leuven research university in Leuven, Belgium, broke the SIKE algorithm in about 62 minutes. They did it using a single core on a six-core Intel Xeon CPU E5-2630v2 at 2.60GHz, according to their article, An Efficient Key Recovery Attack On SIDH.

KyberSlash: division timings depending on secrets in Kyber software

Introduction | Libraries | FAQ

Various Kyber software libraries in various environments leak secret information into timing, specifically because

- these libraries include a line of code that divides a secret numerator by a public denominator,
- the number of CPU cycles for division in various environments varies depending on the inputs to the division, and
- this variation appears within the range of numerators used in these libraries.

The KyberSlash pages track which Kyber libraries have this issue, and include a FAQ about the issue.

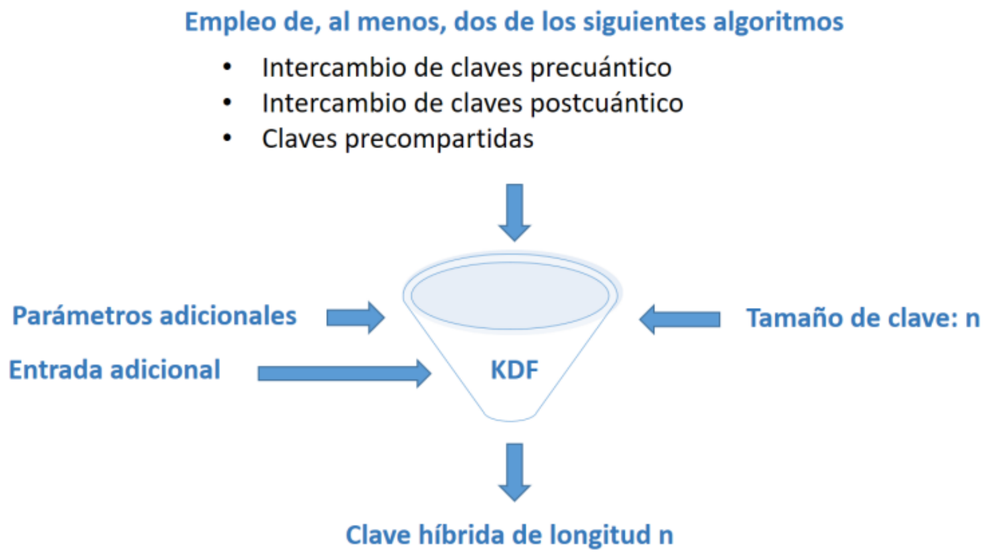
But...

ÍNDICE

ESQUEMAS HÍBRIDOS

Lo mejor de dos mundos

- Los algoritmos asimétricos post-cuánticos resisten a la computación cuántica
- Los algoritmos asimétricos clásicos tienen resistencia demostrada frente a computación clásica
- **Solución: usar ambos de la mano**



PQC CCN - ESPAÑA

Criptosistema asimétrico y KEM	Primitiva matemática
CRYSTALS-Kyber	Retículo estructurado (MLWE)
FrodoKEM	Retículo no estructurado (LWE)

Tabla 4. Algoritmos KEM recomendados por el CCN y primitivas matemáticas asociadas

Firma digital	Primitiva matemática
CRYSTALS-Dilithium	Retículo estructurado (MLWE)
Falcon	Retículo estructurado (SIS)
SPHINCS+	Funciones hash

Tabla 5. Esquemas de firma recomendados por el CCN y primitivas matemáticas asociadas

ESQUEMAS HÍBRIDOS Y PLANES DE MIGRACIÓN

PLANES DE MIGRACIÓN CCN

FASE 1	• Empleo inmediato de las firmas basadas en hash para actualizaciones de firmware.
FASE 2	• Uso de soluciones híbridas para proporcionar mayor defensa a la criptografía precuántica
FASE 3	• Empleo de soluciones híbridas con las garantías de seguridad proporcionadas por la criptografía postcuántica.
FASE 4	• Adopción de los algoritmos criptográficos postcuánticos considerados resistentes a la computación cuántica.

ÍNDICE

CONCLUSIONES

- Los ordenadores cuánticos no hacen magia
- La criptografía asimétrica actual es vulnerable a ellos
- Soluciones: criptografía post-cuántica + hibridación
- Hay que ponerse las pilas!