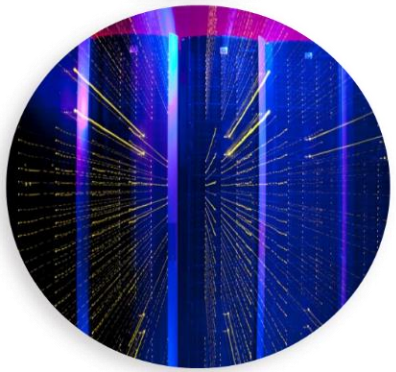
Computación cuántica y HPC. Presente y futuro

Sesión de Tecnologías Emergentes en las JJTT 2023
Zaragoza, 14 de junio de 2023

Andrés Gómez Tato
Fundación CESGA

CESGA
GALICIA SUPERCOMPUTING CENTER

¿Qué es el CESGA?



Misión

Contribuir al avance de la **Ciencia** y de la **Técnica** mediante la **Investigación** y la **Aplicación** de la **Computación** y las **Comunicaciones** de **altas prestaciones**, en **colaboración** con otras instituciones, para beneficio de la **Sociedad**.

Servicios

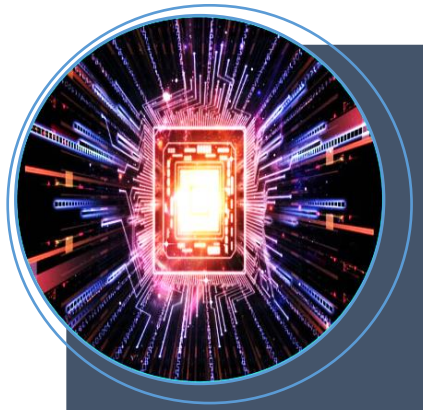
Adaptados a la evolución tecnológica y a las necesidades de los investigadores y usuarios de cualquier área de conocimiento o sector productivo.

RETOS ACTUALES Y FUTUROS

Big Data, Industry 4.0

IA: ML y **DL** Necesidad de gran cantidad de computación y alomacenamiento. HPC es una herramienta fundamental para ser competitivo

CESGA: Proporciona herramientas para reducir el esfuerzo de empleo de ML usando HPC



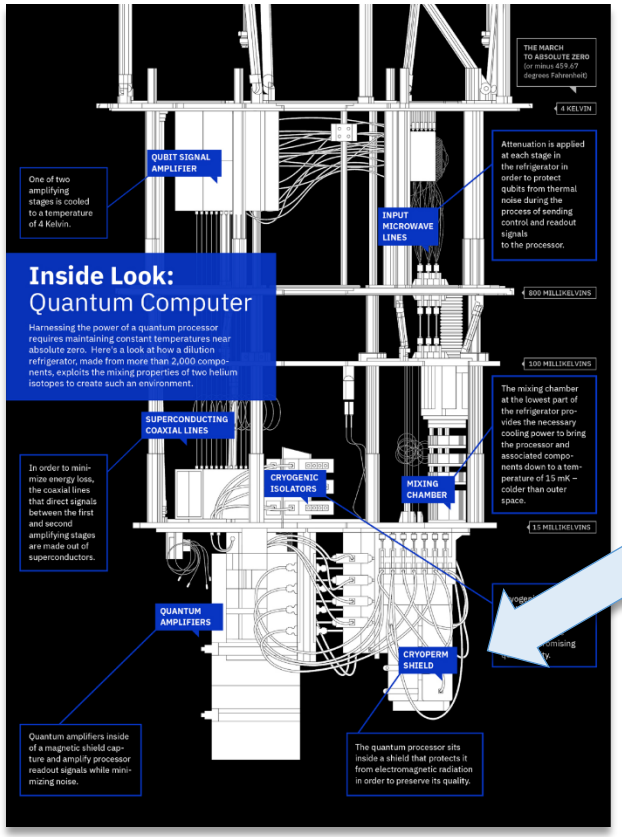
Futuro: Computación y Comunicaciones Cuánticas

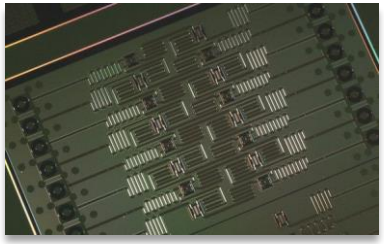
CESGA
GALICIA SUPERCOMPUTING CENTER

¿Qué es la computación cuántica?

Computación cuántica. ¡Bienvenidos a un sueño!

Yuri Manin (1980) y Richard Feynman (1981) propusieron de forma independiente la Computación Cuántica





I'm here very "hot"!!
-273ºC

Source: IBM

https://en.wikipedia.org/wiki/Timeline_of_quantum_computing

Computación cuántica

Una posible definición:

"La computación cuántica es una rama de la computación que usa los principios de la física cuántica para calcular o computar"

Unidad básica de información: Qúbit o cúbit

"un sistema cuántico con dos estados propios y que puede ser manipulado arbitrariamente" (Fuente:Wikipedia)

Es decir:

"un sistema cuántico que cuando lo medimos podemos obtener dos posibles resultados con cierta probabilidad cada uno, que equiparamos al 0 y 1 de los bits clásicos y que podemos manipular, por ejemplo, cambiando las probabilidades de las medidas o cambiando la fase relativa"

Computación cuántica

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

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

Superposición

Números complejos

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

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

Medida:

$|0\rangle$ con probabilidad $|\alpha|^2$ → si volvemos a medir inmediatamente, obtendremos $|0\rangle$

o

$|1\rangle$ con probabilidad $|\beta|^2$ → si volvemos a medir inmediatamente, obtendremos $|1\rangle$

Computación cuántica

Para 2 Cubits:

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle + \delta|3\rangle$$

Para N Cubits:

$$|\psi\rangle = \sum_{i=0}^{2^N-1} \lambda_i |i\rangle$$

1. **Por cada cúbit que añadamos, duplicamos la información que podemos manipular.**
2. **¡Podemos manipular todos los $|i\rangle$ en paralelo!**

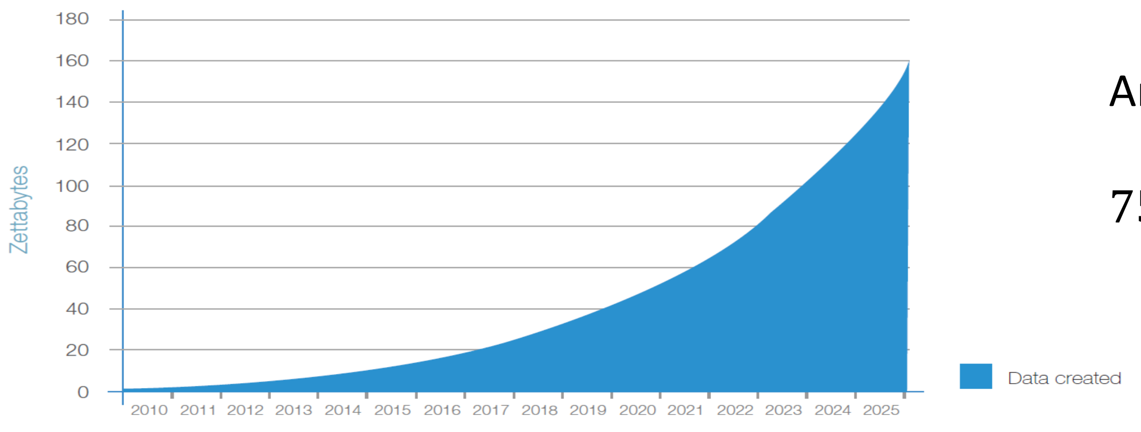
Computación cuántica

Asimov calculó que el número de nucleones+electrones en el Universe as $\sim 10^{79}$

$\sim$ 10.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000

Una QPU con 270 cubits, podría acumular: $\sim 4{\cdot}10^{81}$ números reales (2 por cada número complejo).

Figure 2. | Annual Size of the Global Datasphere



Source: IDC's Data Age 2025 study, sponsored by Seagate, April 2017

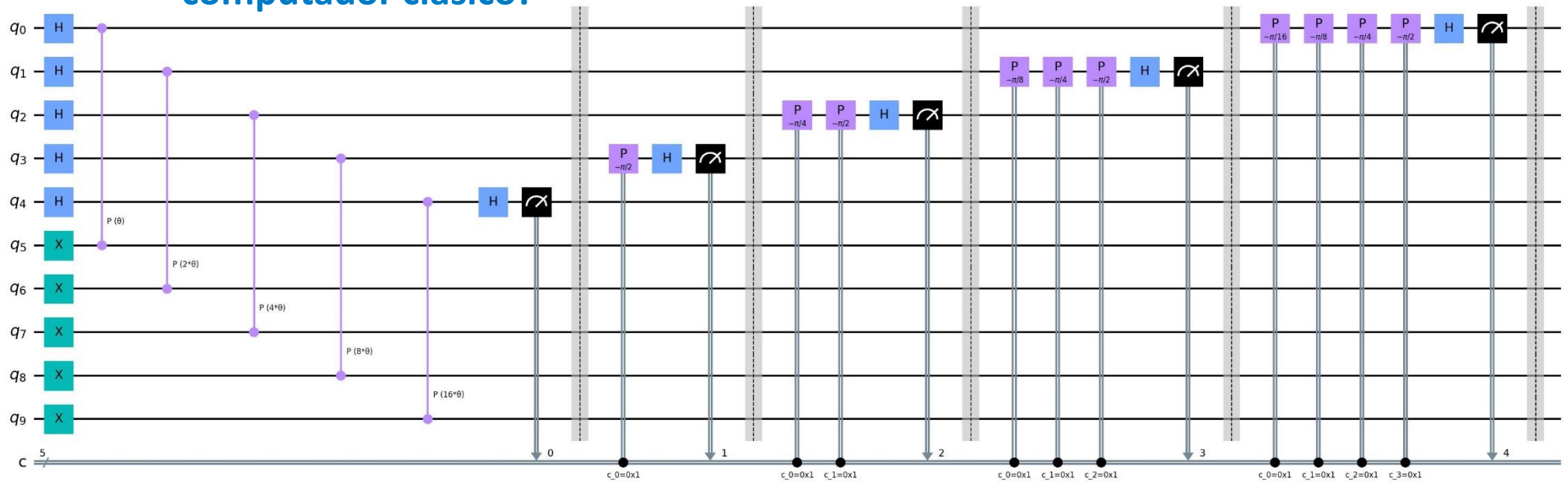
Año 2025: $\sim$170ZB/año $\sim 10^{23}$ bytes/año

75 cubits: $\sim 6{\cdot}10^{23}$ bytes

Computación cuántica

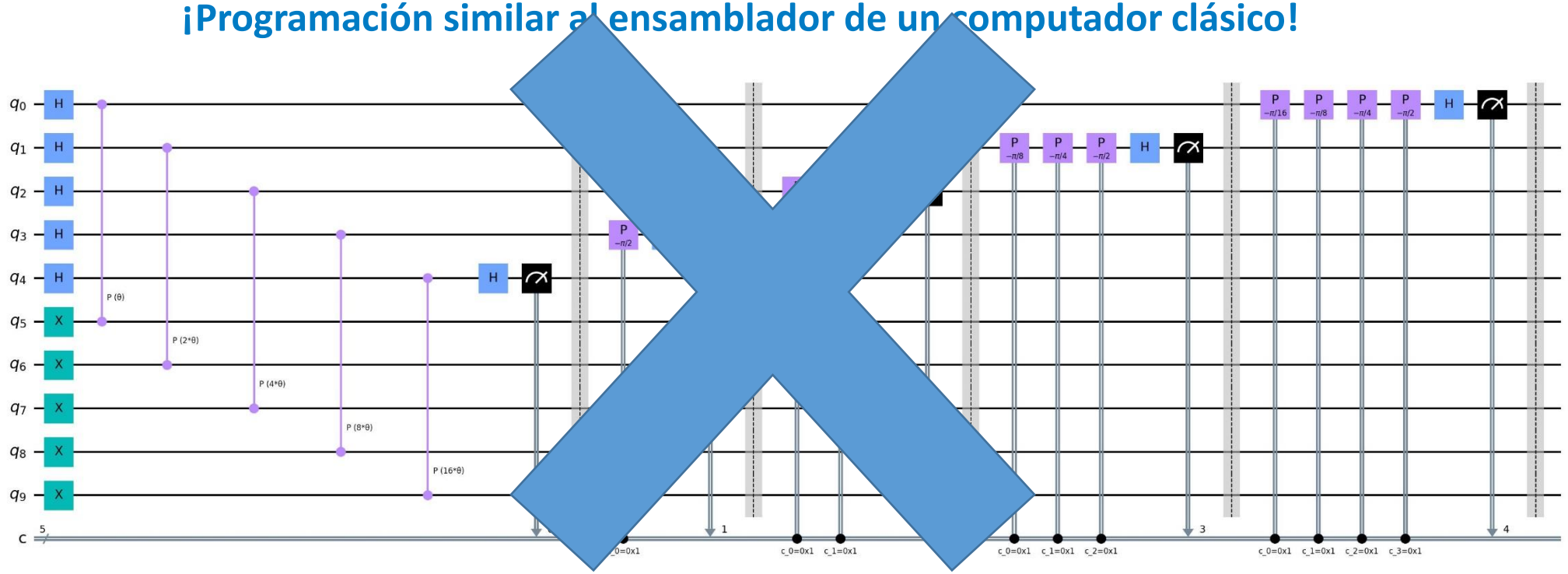
30 Aniversario CESGA
GALICIA SUPERCOMPUTING CENTER

¡Programación similar al ensamblador (o incluso, microcódigo) de un computador clásico!



Computación cuántica

¡Programación similar al ensamblador de un computador clásico!

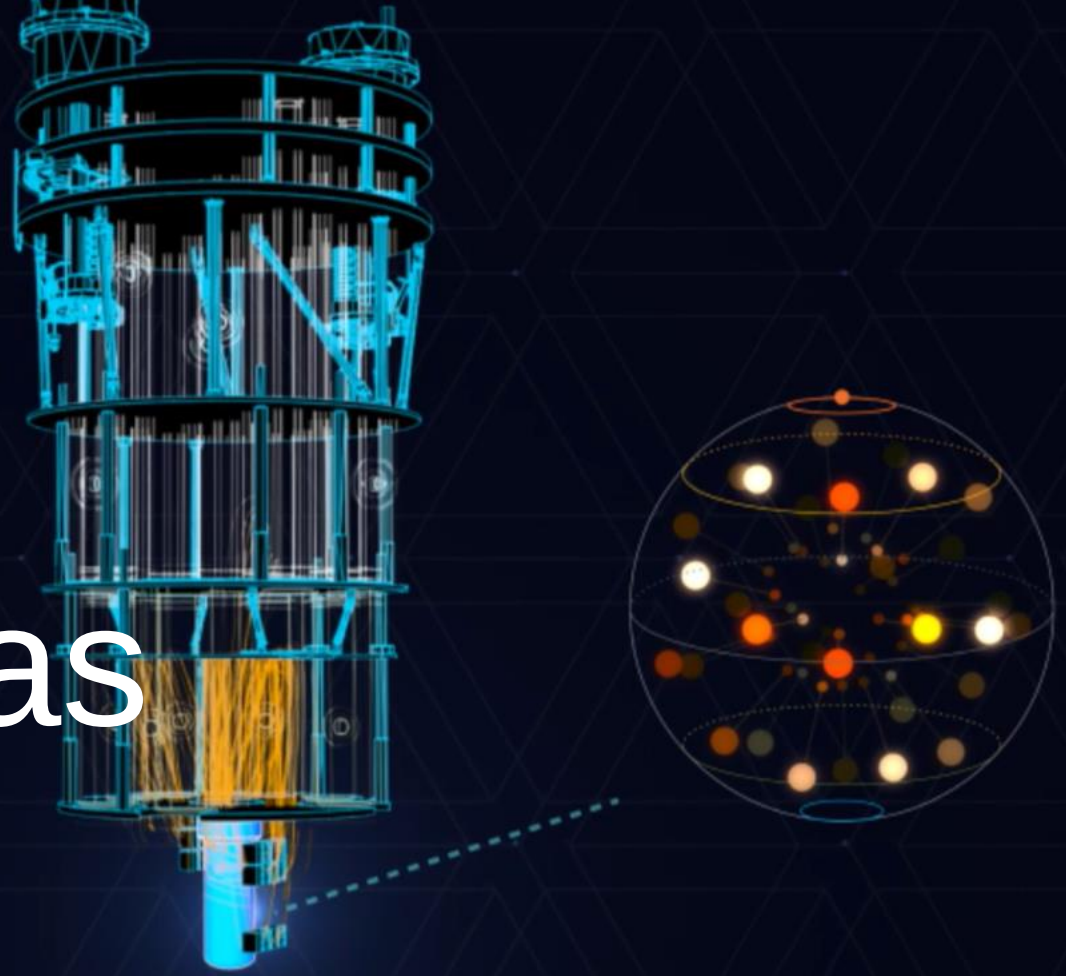


HAY LIBRERIAS DE ALTO NIVEL PARA MUCHOS CAMPOS:

- **QUÍMICA**
- **FINANZAS**
- **QUANTUM MACHINE LEARNNING….**

CESGA
GALICIA SUPERCOMPUTING CENTER

¿Computadoras Cuánticas?



Computadores Cuánticos

No hay un único modelo de computación cuántica:

- Computador cuántico digital.
- Simulador cuántico.
- Computador analógico-digital.
- Computación Adiabática.
- Etc.

NO, no va a multiplicar más rápido (al menos a corto plazo)

- Es una nueva forma de algoritmia.
- Orientada a resolver problemas específicos, difíciles en computación clásica.
- Actualmente, mejor si no tienen muchos datos de entrada.

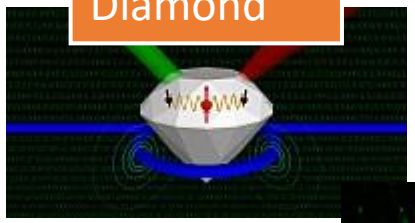
Computadores Cuánticos

No hay un único hardware:

Ion Trap

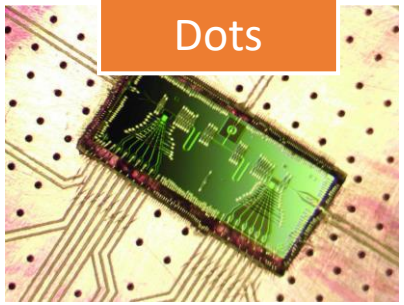
Transmon

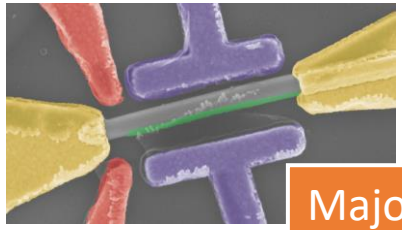
NV-Defect Diamond



Photons

Quantum Dots





Majorana?

And more ....

Computadores Cuánticos

Posibles ventajas (por demostrar empíricamente):

- Resolver problemas que un computador clásico no podría (*Supremacía Cuántica*). Ejemplo: romper las claves de RSA[1] (Algoritmo de Shor).
- Obtener una solución mejor que los algoritmos clásicos. Ejemplo: Optimización en logística. Quantum Machine Learning.
- Obtener una solución igual o equivalente, pero en menos tiempo.
- Obtener una solución igual, equivalente o incluso ligeramente peor (pero usable), consumiendo menos energía

Todos los algoritmos son híbridos (cuántico-clásicos)

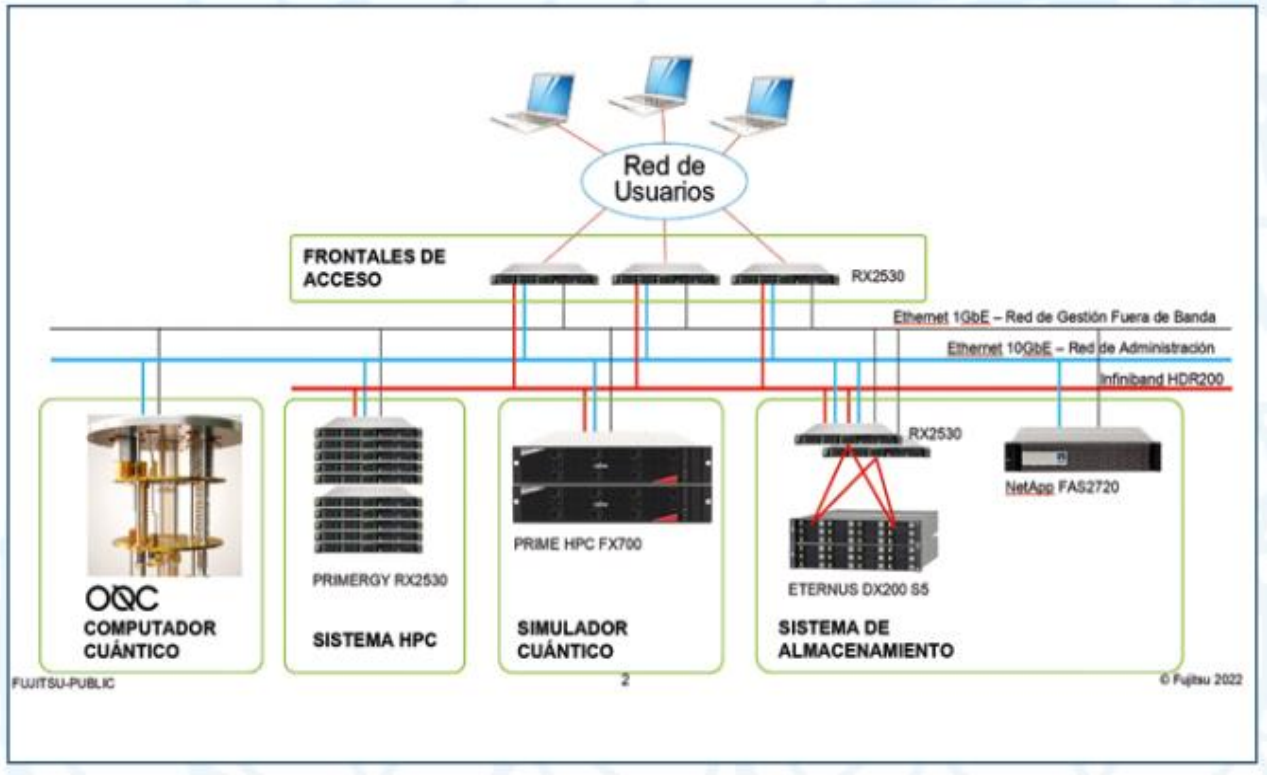
- La escalabilidad de los algoritmos cuánticos puede estar condicionada por la computación clásica (o incluso, no existir).

1. No se conoce ningún algoritmo clásico público que lo permita cuando la clave es suficientemente grande. Pero eso no quiere decir que no exista.

Computadores Cuánticos. CESGA

Despliegue de un computador cuántico:

- En proceso de despliegue.
- **32 cubits**
- Disponible en septiembre de 2023.
- Orientado a la investigación.



Despliegue de una infraestructura basada en tecnologías cuánticas de la información que permita impulsar la I+D+i en Galicia. Operación financiada por la Unión Europea, a través del FONDO EUROPEO DE DESARROLLO REGIONAL (FEDER), como parte de la respuesta de la Unión a la pandemia de la COVID-19.
PROGRAMA OPERATIVO
FEDER
2014-2020

Una manera de hacer Europa

UNIÓN EUROPEA

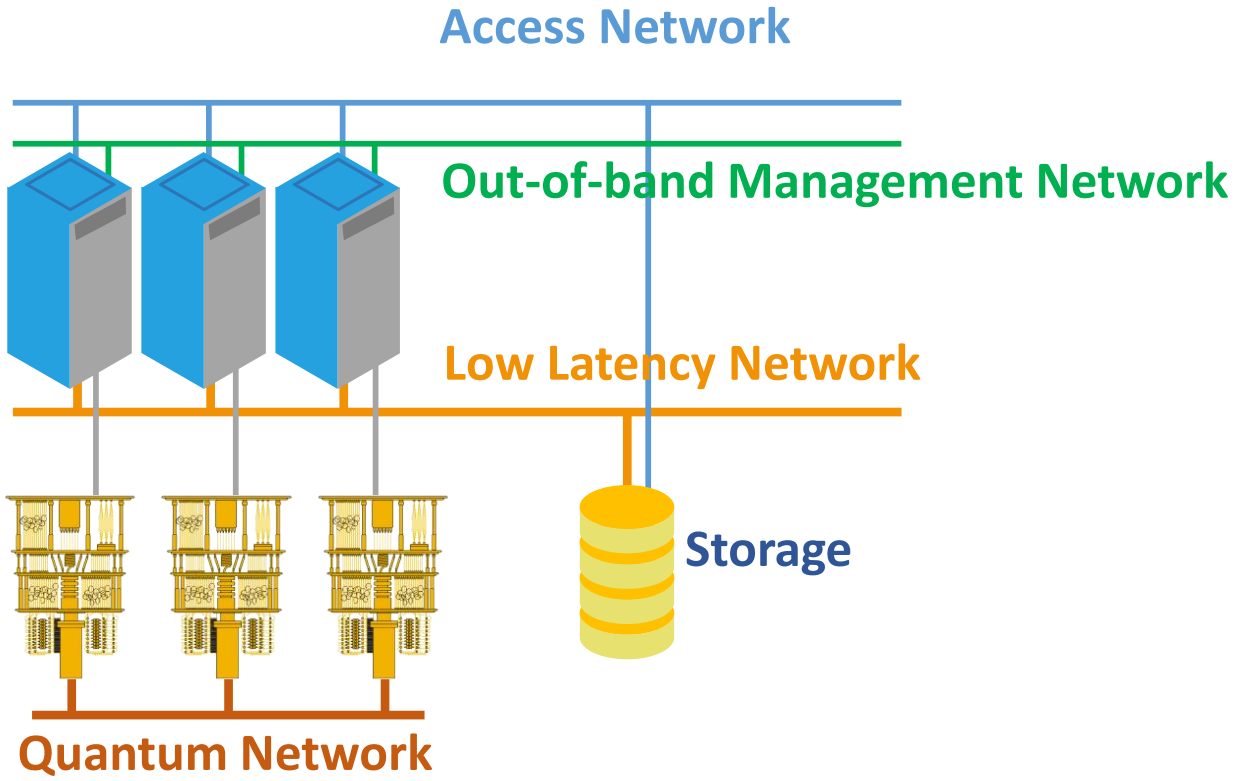
AXENCIA GALEGA DE INNOVACIÓN

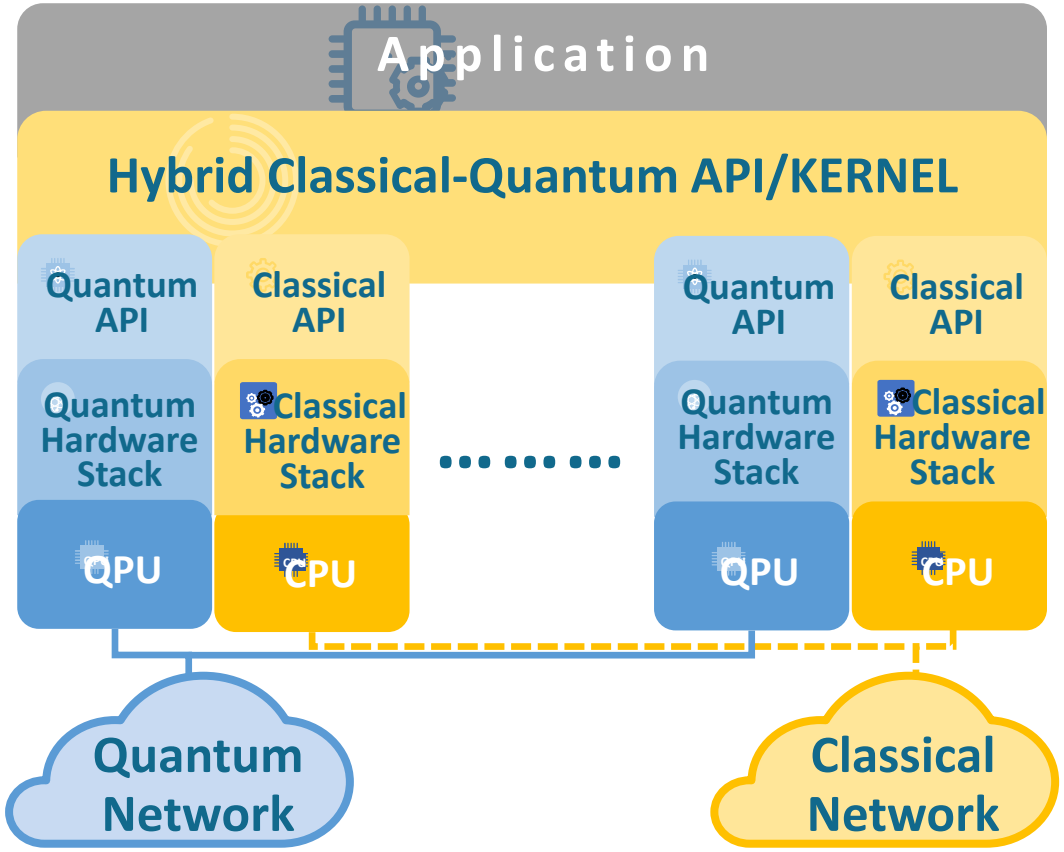
Xacobeo 21·22

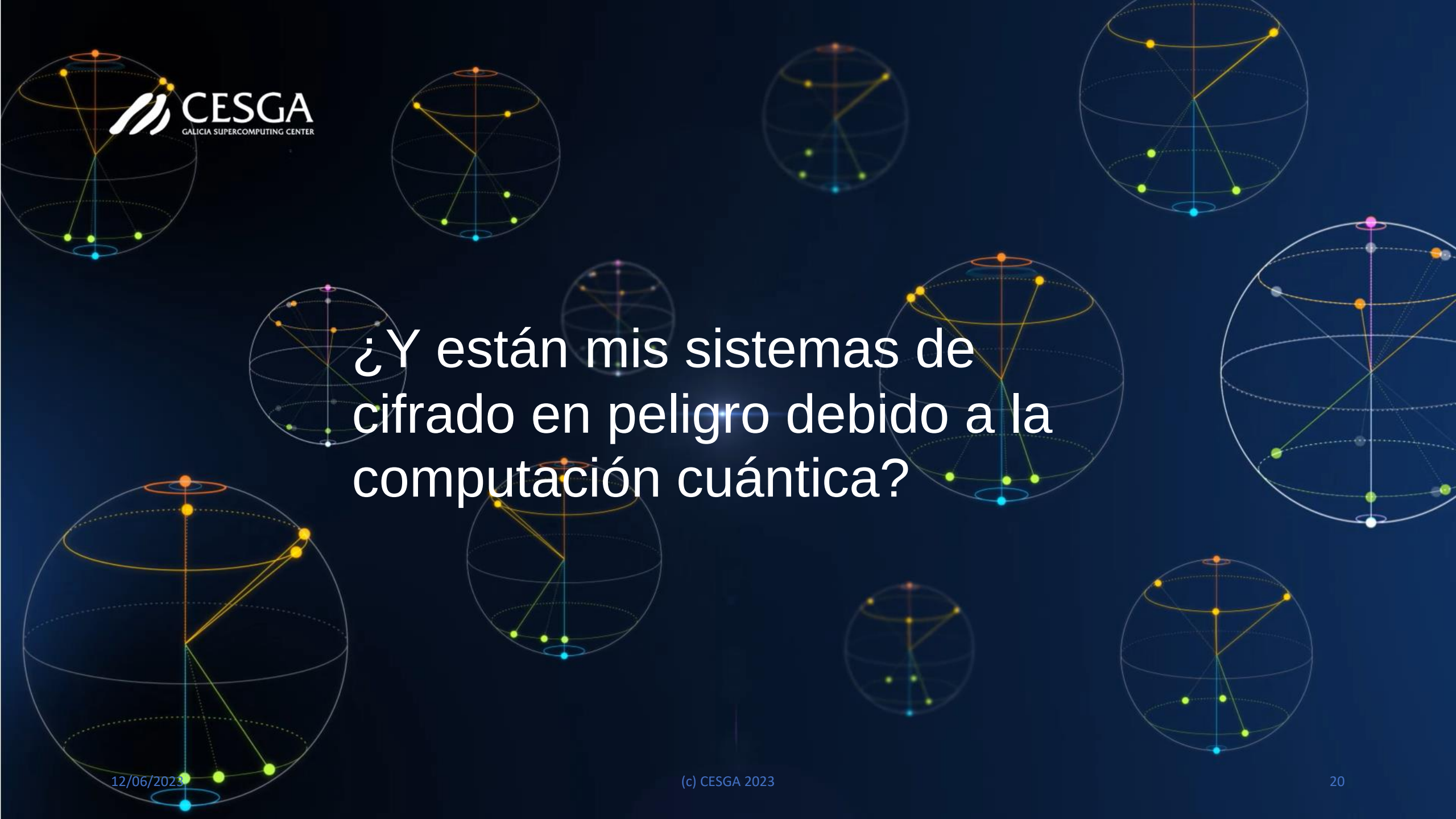
CESGA
GALICIA SUPERCOMPUTING CENTER

Futuro: Computadores Cuánticos de Altas Prestaciones

Futuro: Computadores Cuánticos de Altas Prestaciones







¿Y están mis sistemas de cifrado en peligro debido a la computación cuántica?

¿Computadores Cuánticos romperán RSA?

¿Pueden romper los computadores cuánticos los algoritmos de cifrado? :

- Algoritmo de Shor.
- Variational Quantum Factoring.
- Usando Computación Adiabática (como un problema de optimización).
- Algoritmo de Schnorr con aceleración cuántica ← Si realmente funciona, YA se podrían romper las claves de 2048 bits

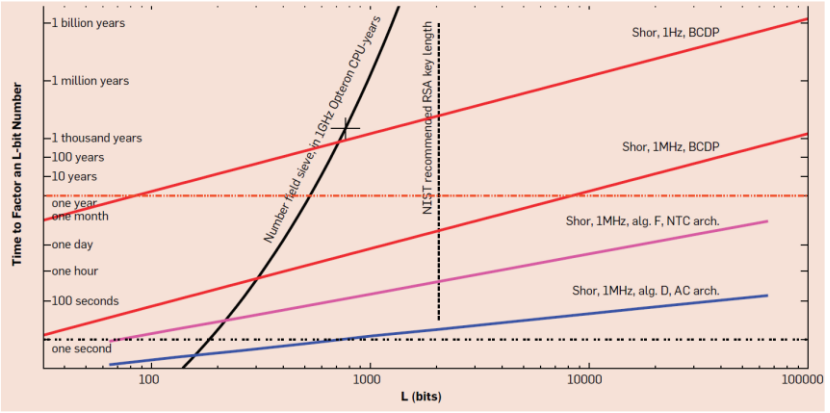
¿Cuándo podrá romperlos usando el algoritmo de Shor? :

- Muy difícil saberlo. Pero mejor, hay que ir pensando en cambiar el algoritmo de firma y cifrado (criptografía post-cuántica).
- **NIST** se hizo eco de una presentación de Matteo Mariantoni en PQCrypto 2014, en donde decía que el primer ordenador cuántico criptográficamente relevante podría construirse en 2030.
- Algoritmo de Shor necesita:
  - Largos tiempos de coherencia (horas/días/semanas). Ahora estamos del orden de segundos o menos.
  - Una mejor conectividad entre cubits.
  - Muchos más cubits. Para claves de 2048 bits, se estima que necesitaremos 20 millones y 8 horas (en el mejor de los casos).
  - Pero, doblando cada año el número de cubits (¿ley de Moore?), partiendo del valor actual 433: **2038**[1]

How a quantum computer could break 2048-bit RSA encryption in 8 hours

MIT Technology Review

A new study shows that quantum technology will catch up with today's encryption standards much sooner than expected. That should worry anybody who needs to store data securely for 25 years or so.



Fuente: Van Meter, R., & Horsman, C. (2013) http://doi.org/10.1145/2494568

1. En mi descargo. NO tomen esto como una predicción seria. No soy vidente y no sé si pasará o no pasará ese año o antes o después. No vaya a pasar como con el directivo de IBM al que se le achacó la frase: " I think there is a world market for maybe five computers" (que además, parece ser una *Fake News* de 1950- http://www-03.ibm.com/ibm/history/documents/pdf/faq.pdf)

g

30 Aniversario CESGA
GALICIA SUPERCOMPUTING CENTER

Actividades financiadas por:

Plan Complementario de Comunicaciones Cuánticas:

- Fondos Next Generation EU (MRR)

GOBIERNO DE ESPAÑA MINISTERIO DE CIENCIA E INNOVACIÓN

ESPAÑA PUEDE. PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y RESILIENCIA

Financiado por la Unión Europea NextGenerationEU

This work was supported by MICIN with funding from the European Union NextGenerationEU (PRTR-C17.I1) and with own funding from the Galician Regional Government through the "Planes Complementarios de I+D+I con las Comunidades Autónomas" in Quantum Communication.

- Fondos propios de la Xunta de Galicia a través de la Axencia Galega de Innovación

AXENCIA GALEGA DE INNOVACIÓN

Subvencionado por la Axencia Galega de Innovación.

CESGA
GALICIA SUPERCOMPUTING CENTER

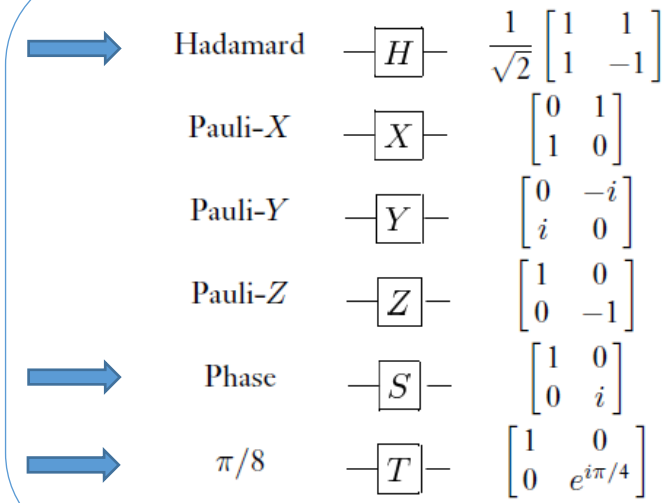
¡GRACIAS!

andres.gomez.tato@cesga.es

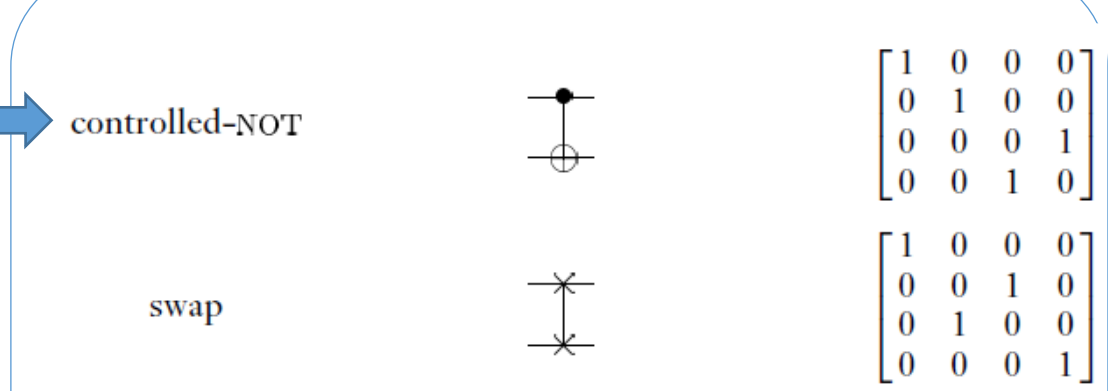
Computación cuántica

¡HAY MAS PUERTAS POSIBLES! EN FUNCIÓN DEL HARWARE UTILIZADO, SE UTILIZA UN CONJUNTO DE PUERTAS DIFERENTES

PUERTAS DE 1 CÚBIT



PUERTAS DE 2 CuBITS



(H,S,T,CNOT) = **Universal Quantum Gates: PUEDE APROXIMAR CUALQUIER OPERACIÓN**