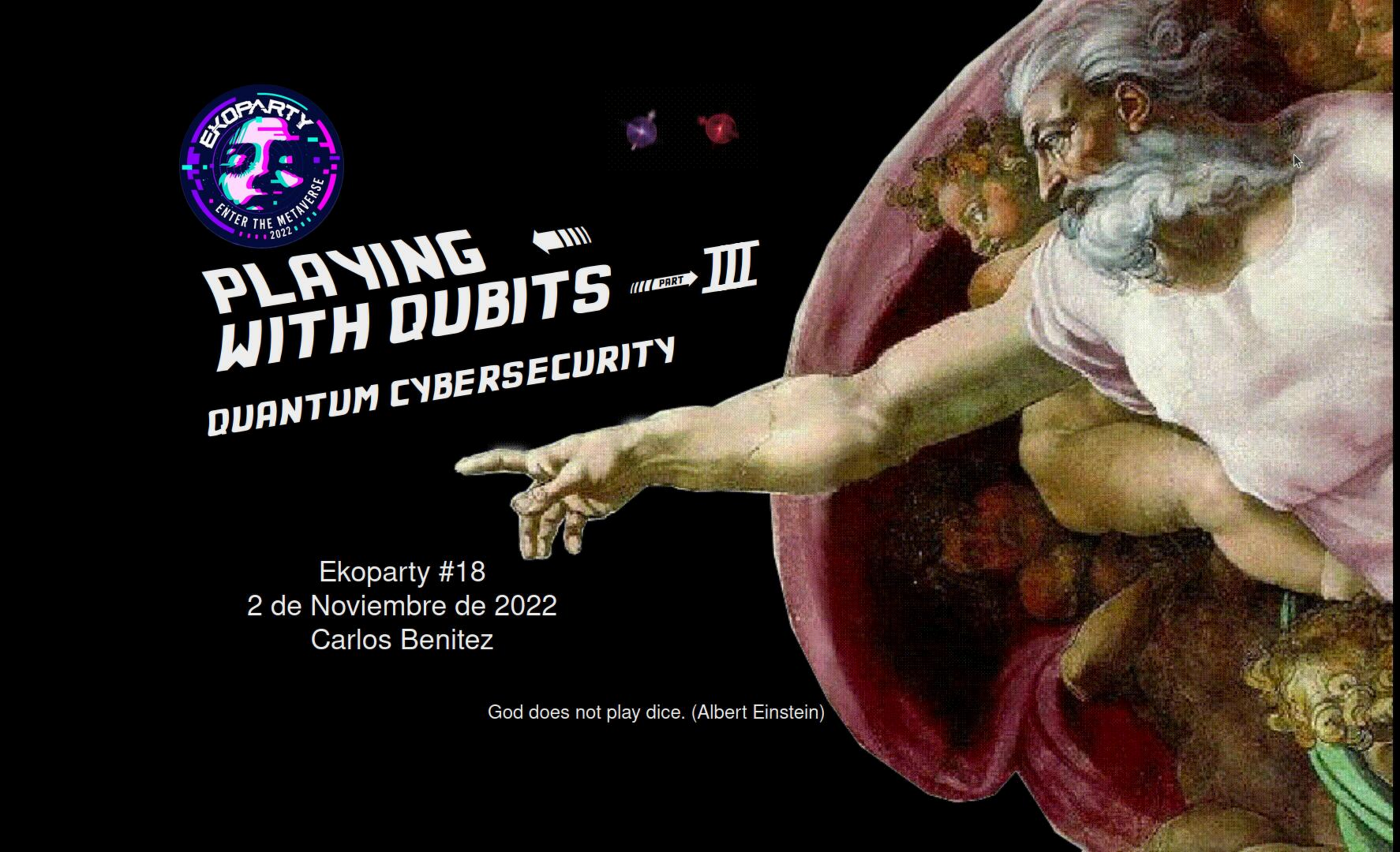


PLAYING WITH QUBITS PART III

QUANTUM CYBERSECURITY

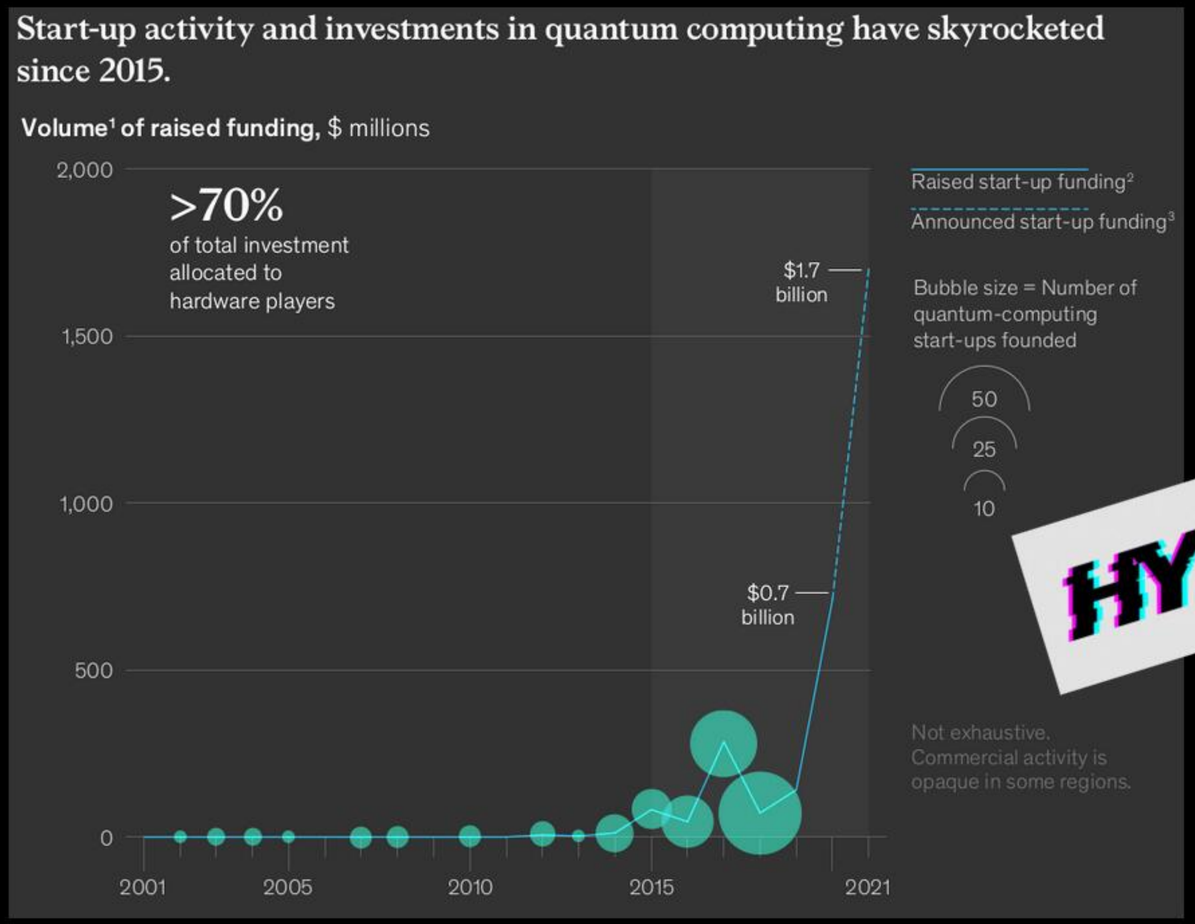
Ekoparty #18
2 de Noviembre de 2022
Carlos Benitez

God does not play dice. (Albert Einstein)

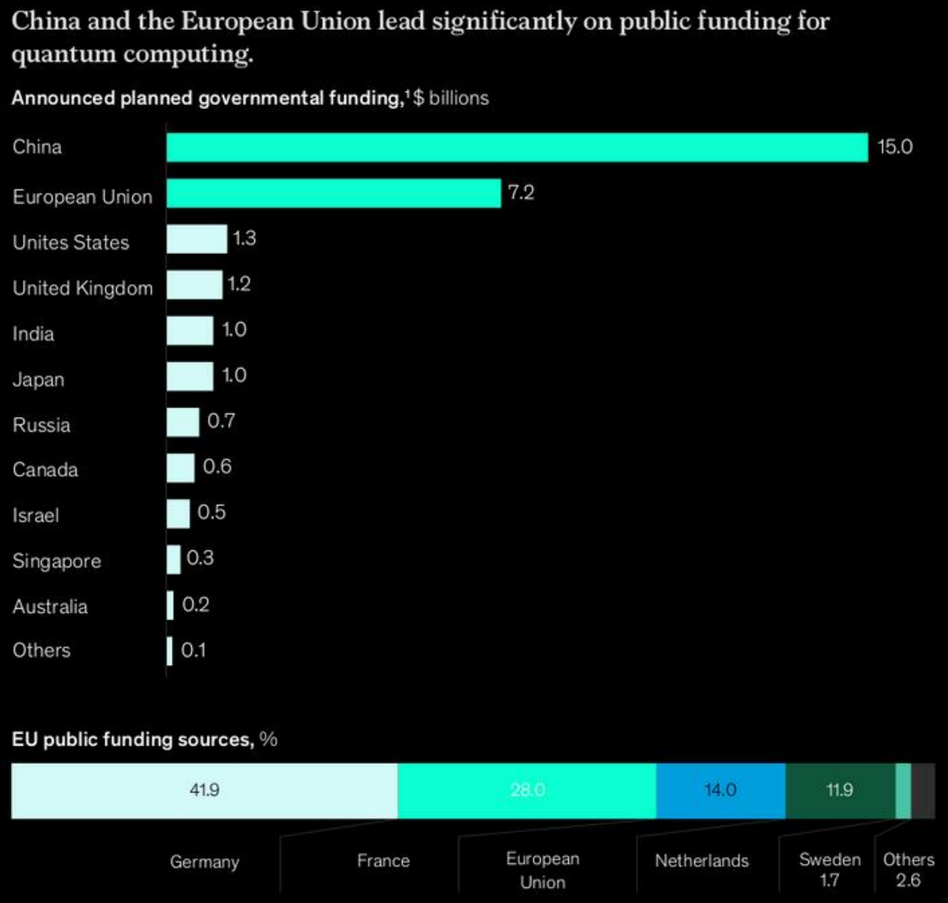
Carlos Benitez

- Ing. y Mg. de la UTN FRBA
- Investigador en procesamiento de señales acústicas submarinas.
- Director del primer Laboratorio en Seguridad Informática (Si6) en el ámbito del Estado.
- Implementación del primer SOC del Ministerio de Defensa.
- Asesor técnico de la Subsecretaría de Ciberdefensa.
- Consultor en ciberseguridad.
- Co-fundador de Platinumciber.
- Proyectos de ciberseguridad, como: SOC, Ethical Hacking, Vulnerability Assessment, Análisis forense, Análisis y Gestión de Riesgos, etc.
- Algunas publicaciones en congresos y una patente en USA en ciberseguridad.
- Docente de posgrado en ciberseguridad.
- Formador y mentoring de teams.
- **Quantum Computing enthusiast.**

WHO AM I?



HABLEMOS DE NUMEROS



HABLEMOS DE NUMEROS

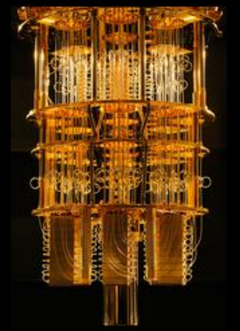
Luciano Bello

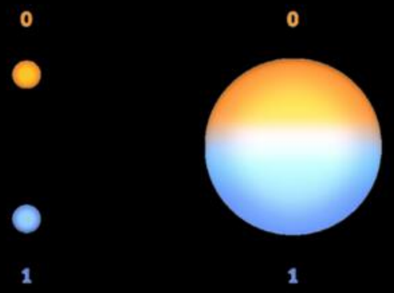
Fernando Virdia

AGRADECIMIENTOS


PREVIOUSLY

PLAYING WITH QUBITS \
CONCEPTOS COMPUTACION CUANTICA



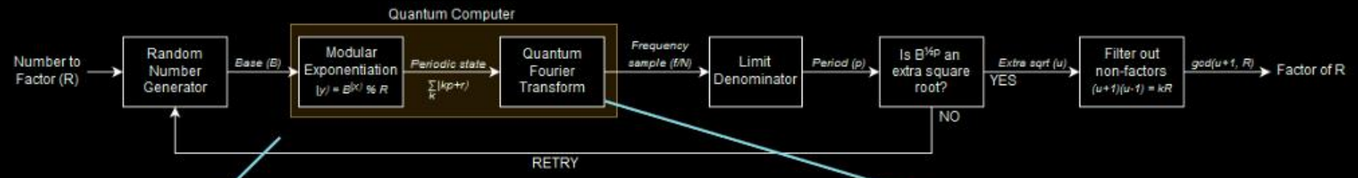


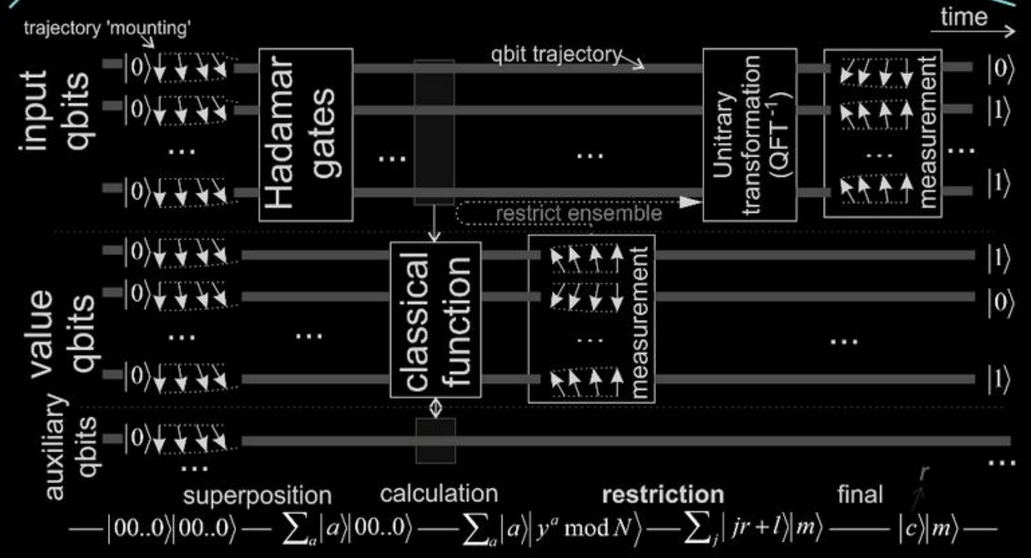
x	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$
0	0	1	1	0
1	1	0	1	0

Is $f(x)$ **balanced** or **constant**?

➠PLAYING WITH QUBITS II

➠EL ALGOTIMO DE SHOR





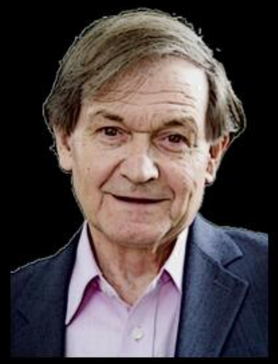
- PLAYING WITH QUBITS
  - CONCEPTOS
    - COMPUTACION CUANTICA
    - CRIPTOGRAFIA POST-CUANTICA
    - *CRIPTOGRAFIA CUANTICA*
  - *COMUNICACION CUANTICA*
- *RESUMEN*

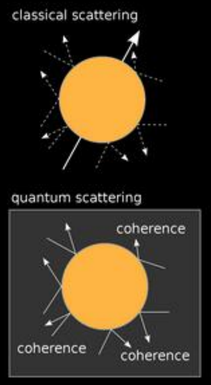
CONCEPTOS

SUPERPOSICION

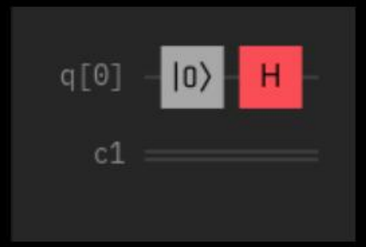

$\frac{1}{\sqrt{2}}|\rangle+\frac{1}{\sqrt{2}}|\rangle$
$|\rangle$
$|\rangle$
SUPERPOSICION

$$\frac{1}{\sqrt{2}}|\text{Garfield}\rangle+\frac{1}{\sqrt{2}}|\text{Garfield}\rangle$$

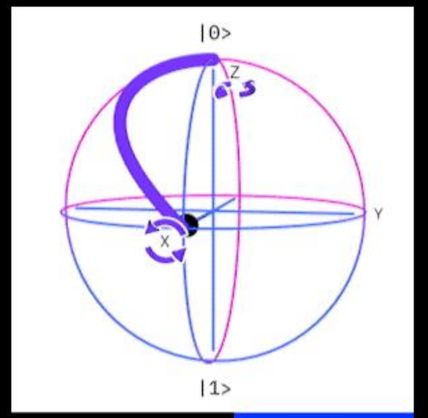




➡ SUPERPOSICION

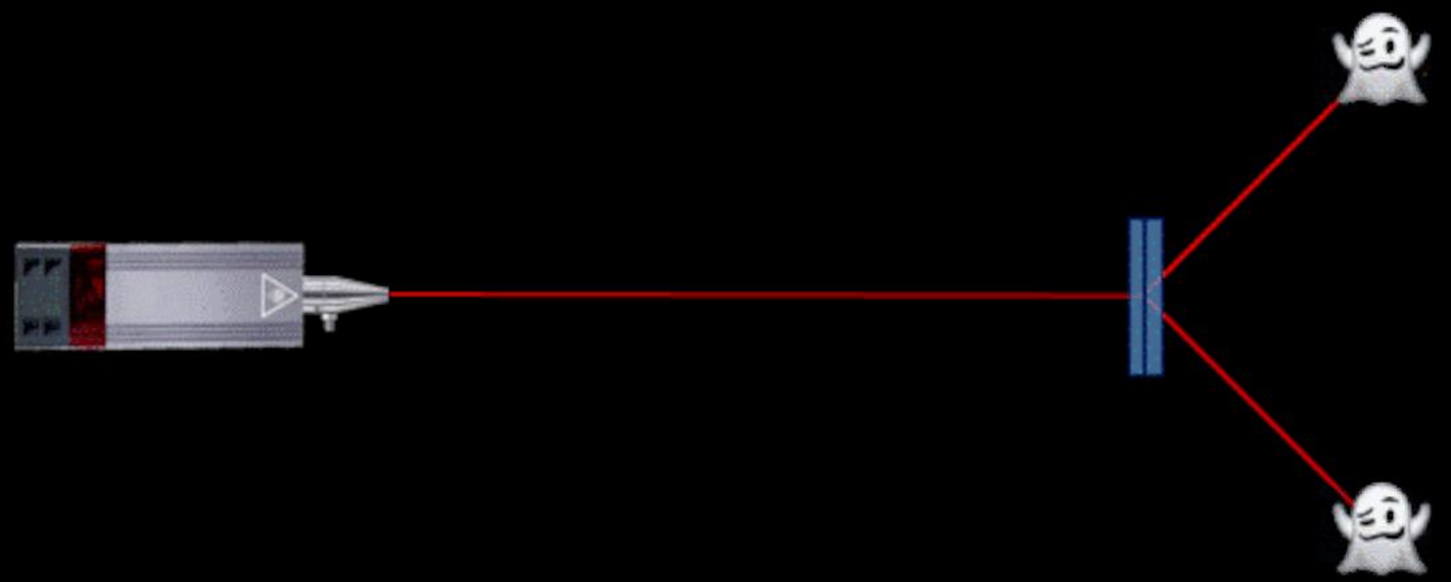


$$H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$



|0⟩ → |+⟩

SUPERPOSICION



ENTANGLEMENT

MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

(Received March 25, 1935)

In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system. In quantum mechanics in the case of two physical quantities described by non-commuting operators, the knowledge of one precludes the knowledge of the other. Then either (1) the description of reality given by the wave function in

1.

ANY serious consideration of a physical theory must take into account the distinction between the objective reality, which is independent of any theory, and the physical concepts with which the theory operates. These concepts are intended to correspond with the objective reality, and by means of these concepts we picture this reality to ourselves.

In attempting to judge the success of a physical theory, we may ask ourselves two questions: (1) "Is the theory correct?" and (2) "I the description given by the theory complete? It is only in the case in which positive answe may be given to both of these questions, that concepts of the theory may be said to be s factory. The correctness of the theory is ju by the degree of agreement between the clusions of the theory and human expe

NEW-YORK, WEDNESDAY, APRIL 28TH 1935

EINSTEIN ATTACKS QUANTUM THEORY

Scientist and Two Colleagues Find It Is Not 'Complete' Even Though 'Correct.'

SEE FULLER ONE POSSIBLE

Believe a Whole Description of 'the Physical Reality' Can Be Provided Eventually.

ENTANGLEMENT

ENTANGLEMENT

Physics Vol. 1, No. 3, pp. 195–200, 1964 Physics Publishing Co. Printed in the United States

ON THE EINSTEIN PODOLSKY ROSEN PARADOX*

J. S. BELL†
Department of Physics, University of Wisconsin, Madison, Wisconsin

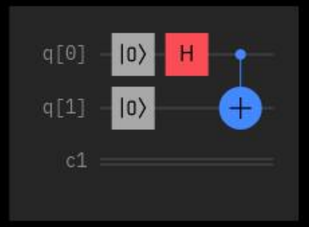
(*Received* 4 *November* 1964)

I. Introduction

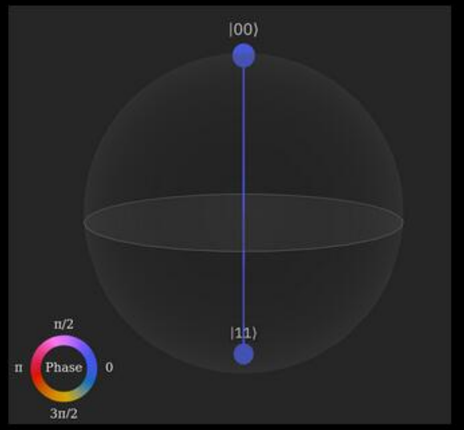
THE paradox of Einstein, Podolsky and Rosen [1] was advanced as an argument that quantum mechanics could not be a complete theory but should be supplemented by additional variables. These additional variables were to restore to the theory causality and locality [2]. In this note that idea will be formulated mathematically and shown to be incompatible with the statistical predictions of quantum mechanics. It is the requirement of locality, or more precisely that the result of a measurement on one system be unaffected by operations on a distant system with which it has interacted in the past, that creates the essential difficulty. There have been attempts [3] to show that even without such a separability or locality requirement no "hidden variable" interpretation of quantum mechanics is possible. These attempts have been examined elsewhere [4] and found wanting. Moreover, a hidden variable interpretation of elementary quantum theory [5] has been explicitly constructed. That particular interpretation has indeed a grossly nonlocal structure. This is characteristic, according to the result to be proved here, of any such theory which reproduces exactly the quantum mechanical predictions.

II. Formulation

With the example advocated by Bohm and Aharonov [6], the EPR argument is the following. Consider

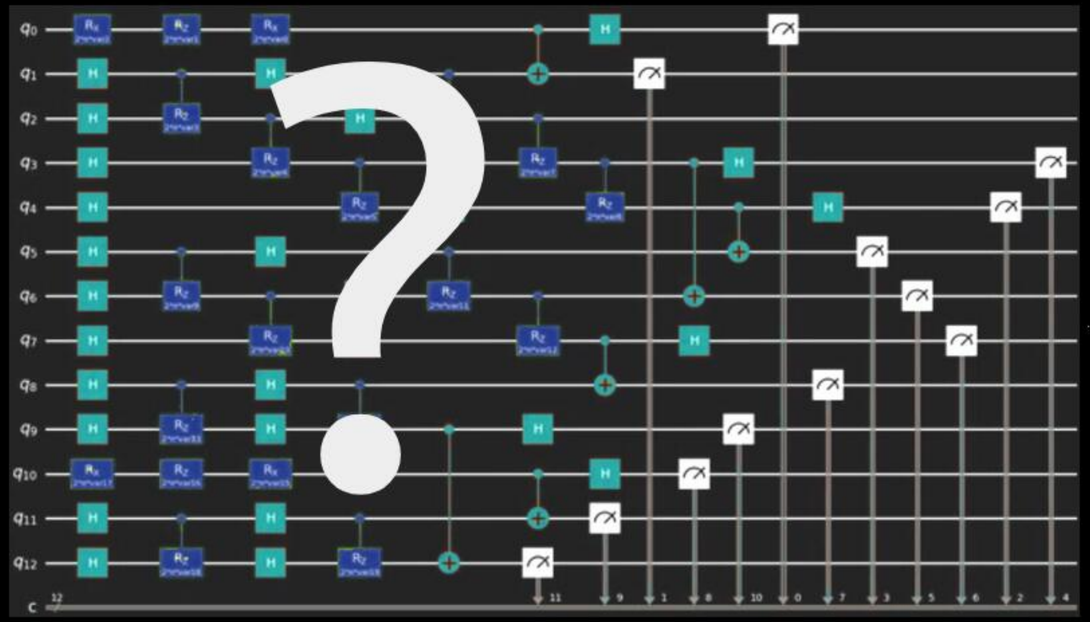


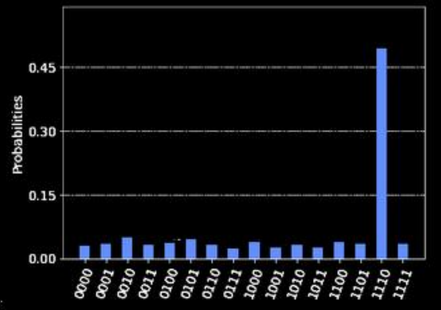
$$H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad \text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

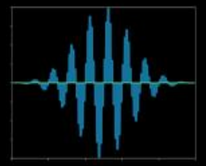


ENTANGLEMENT

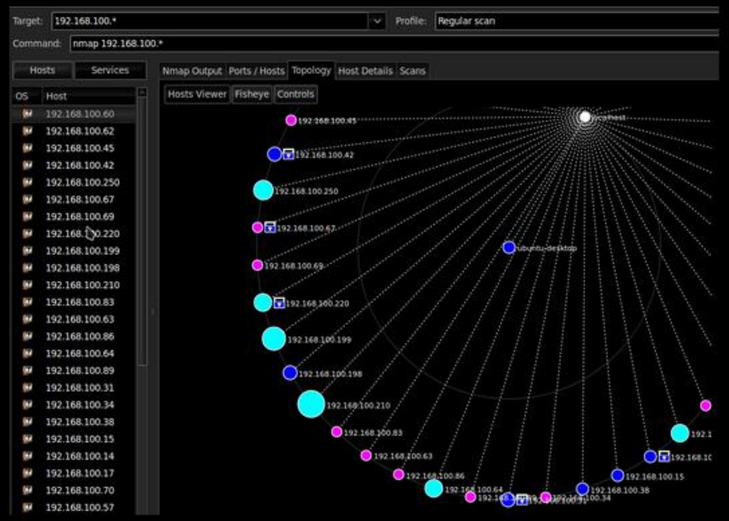
COMPUTACION CUANTICA







CONSIDERACIONES



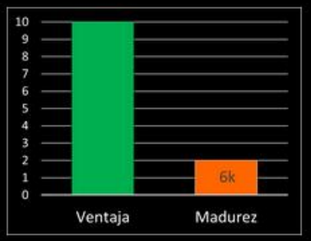
➠LO QUE NO SE PUEDE HACER

➠ LO QUE NO SE PUEDE HACER

RSA

<- Algoritmo de Shor

$$O(N) \rightarrow O\ log(N)$$

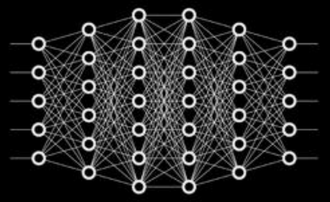


AES

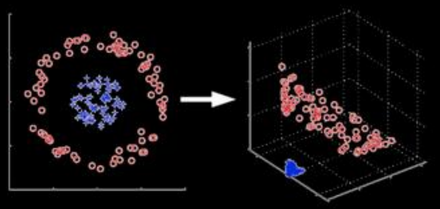
<- Algoritmo de Grover

$$O(N) \rightarrow O(\sqrt{N})$$

➠ LO QUE SI SE PUEDE HACER

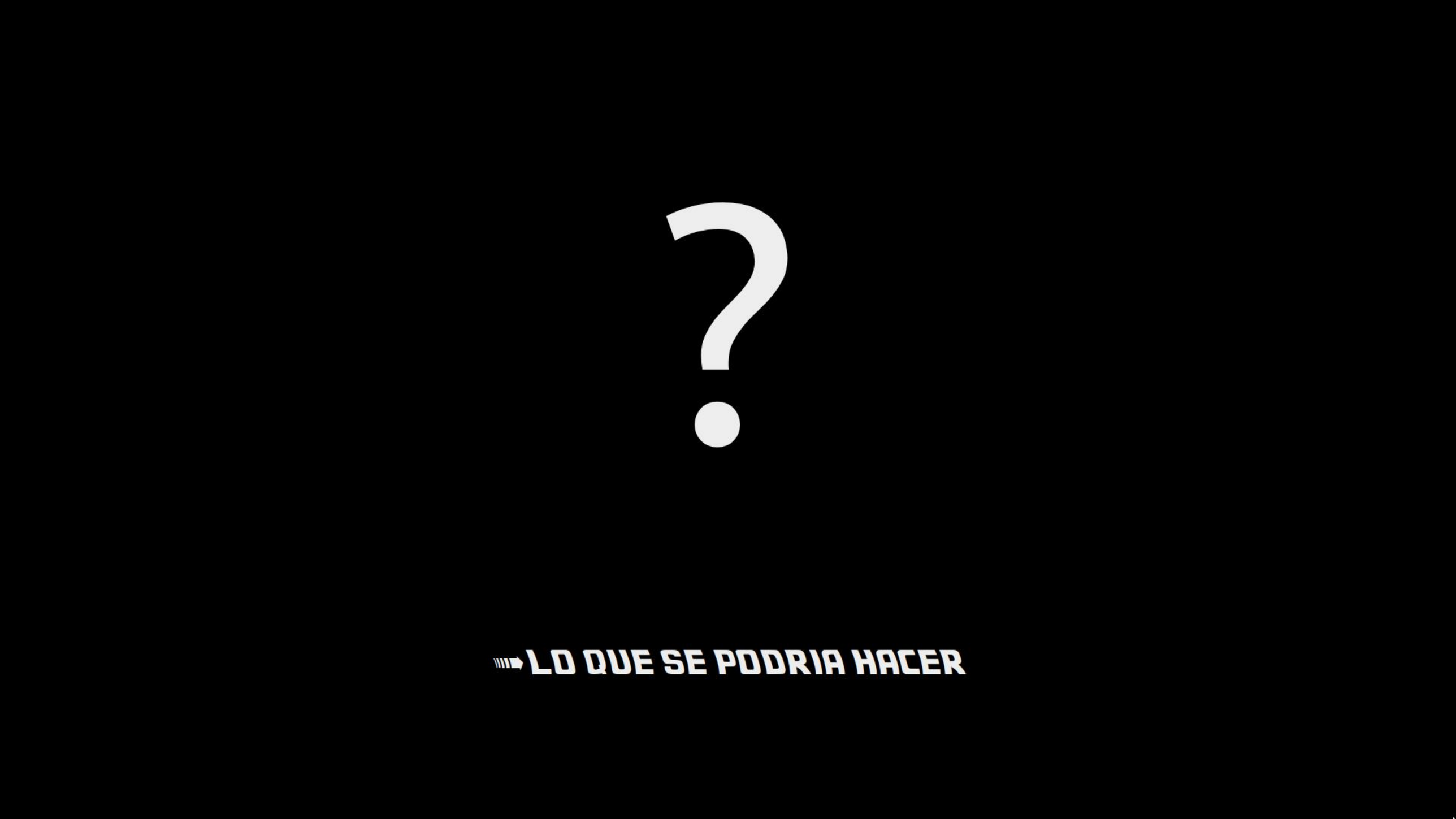


<- QNN



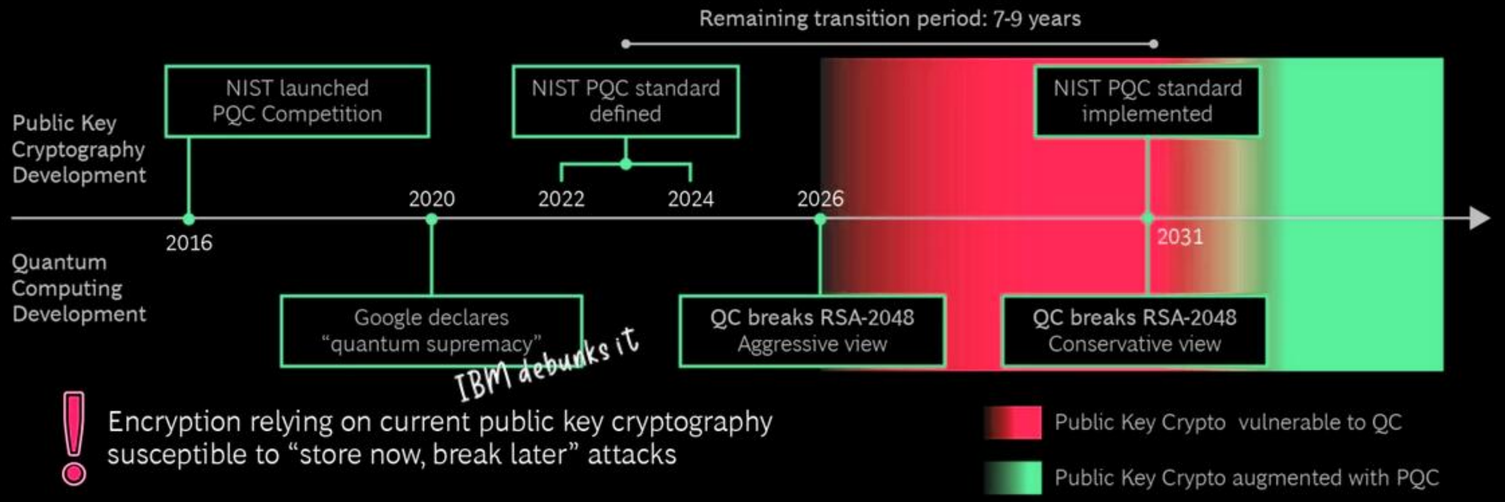
<- QSVM/QKM

➠LO QUE SI SE PUEDE HACER


?
➠LO QUE SE PODRIA HACER

➠CRIPTOGRAFIA POST-CUANTICA

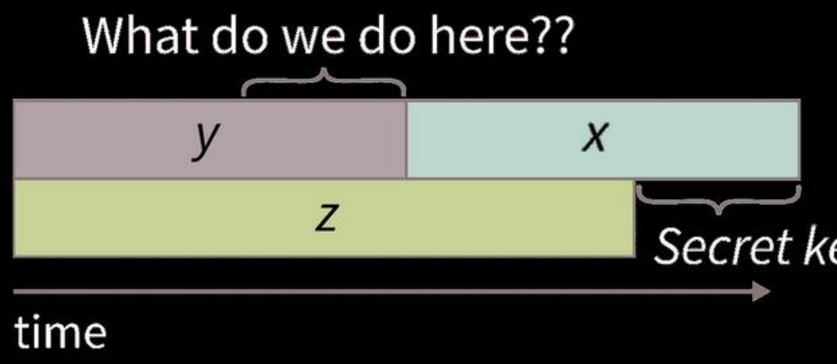
Time Window for Upgrading Cryptographic Infrastructure



➡ LA AMENAZA POST-CUANTICA

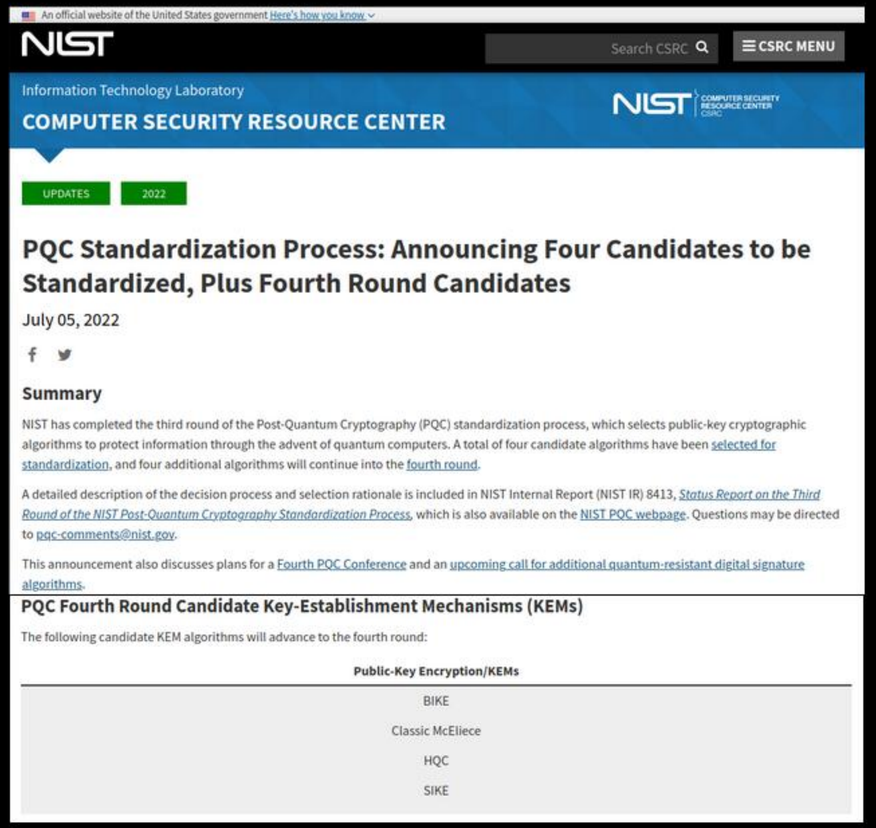
Theorem 1: If $x + y > z$, then worry.

Michele Mosca

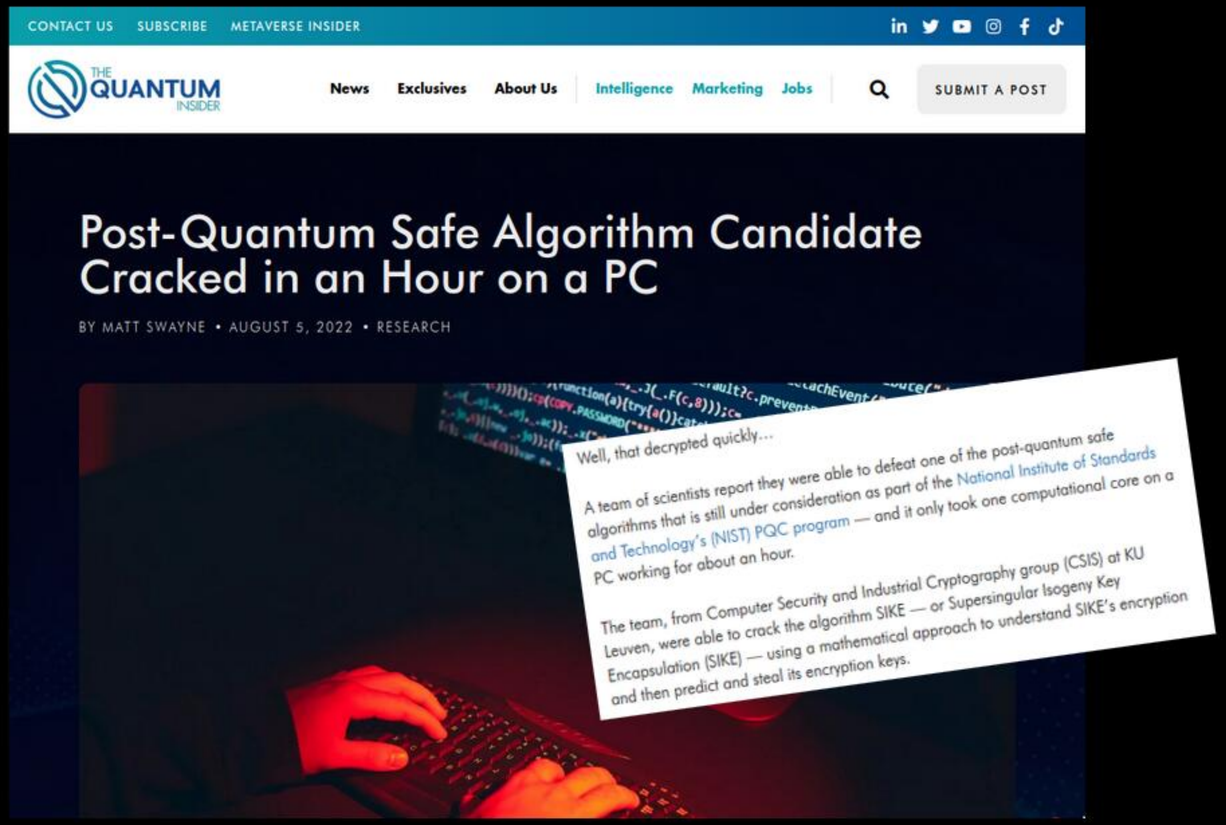


x = período de seguridad de los datos
y = período de transición a PQC
z = tiempo para implementar Shor

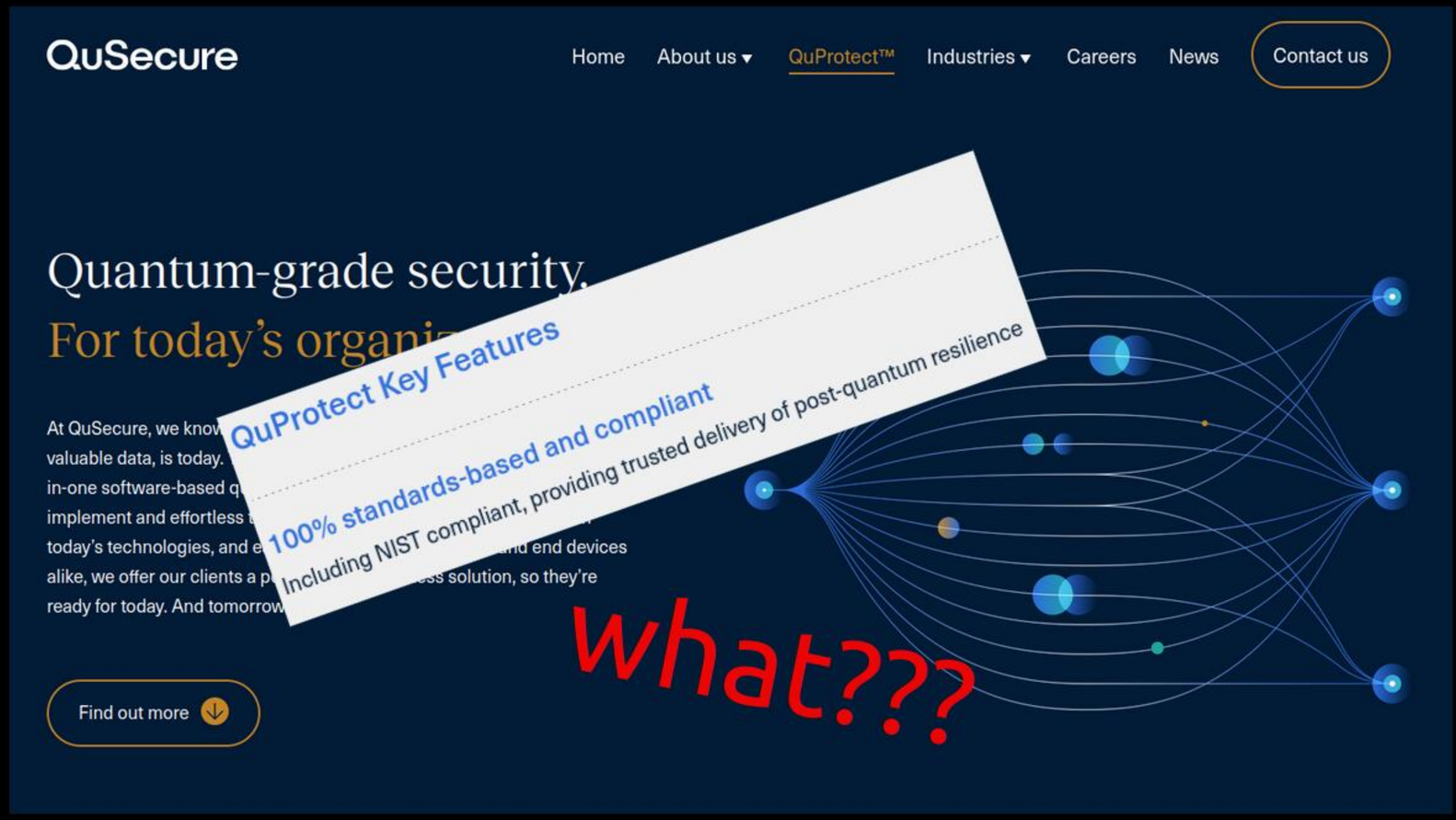
➠ LA AMENAZA POST-CUANTICA



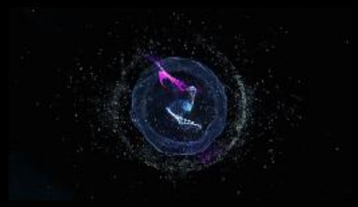
LA COMPETENCIA PQC NIST



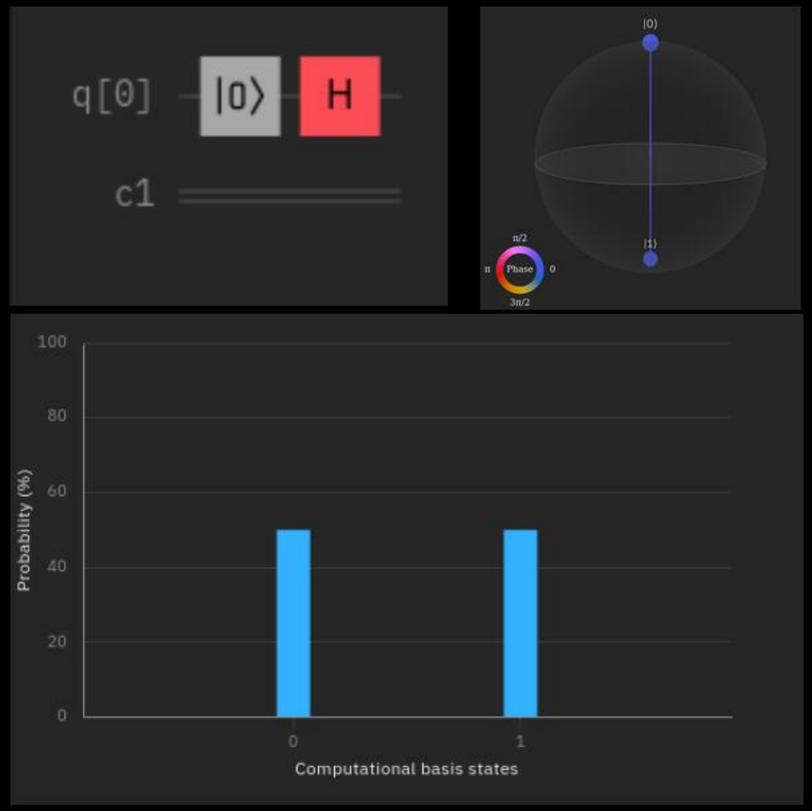
➡ LA COMPETENCIA PQC NIST



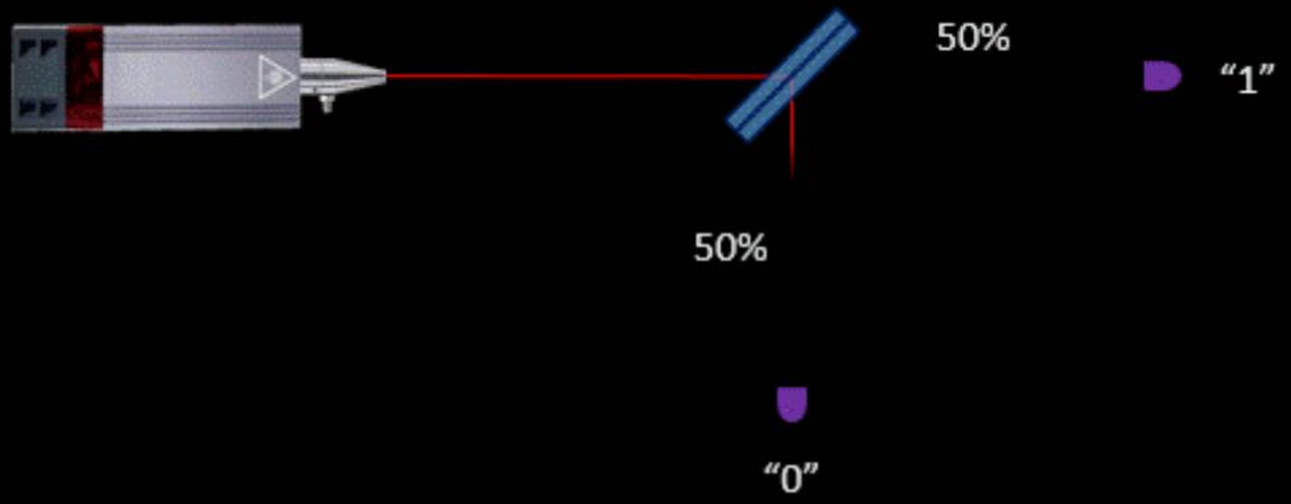
➡ LA AMENAZA POST-CUANTICA



CRIPTOGRAFIA CUANTICA

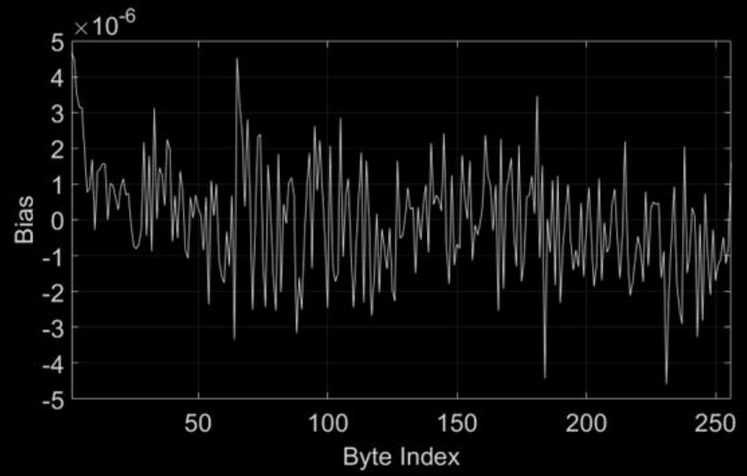


QUANTUM RANDOM NUMBER GENERATION



QUANTUM RANDOM NUMBER GENERATION

Bias!!



➠ QUANTUM RANDOM NUMBER GENERATION

➡QUANTUM KEY DISTRIBUTION

Classic public key criptography

➠QUANTUM KEY DISTRIBUTION

quantum generated keys

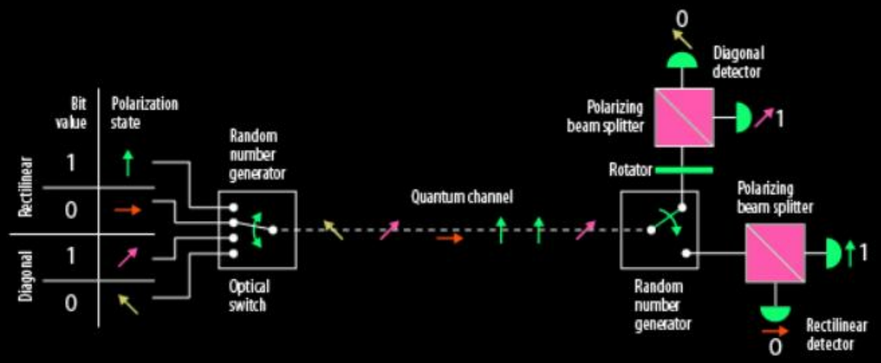
quantum transmission channel

classic encrypted message

classic transmission channel

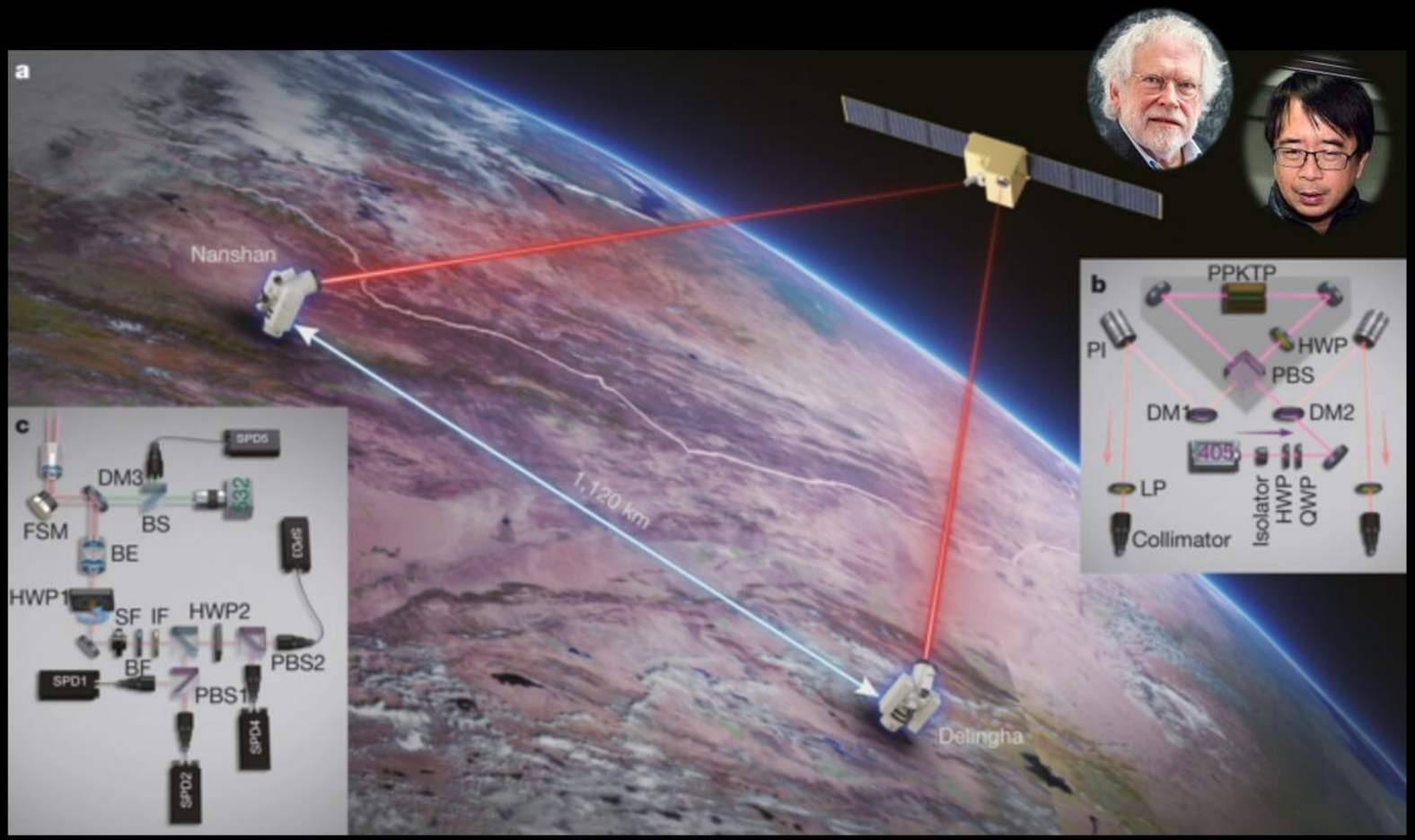
➠QUANTUM KEY DISTRIBUTION

BB84



Quantum transmission & detection	ALICE sends photons	↖	↗	→	↑	↑	↗	↖	↑
	ALICE's random bits	0	1	0	1	1	1	0	1
	BOB's detection events	↑	↗	↖	↑	↗	↗	↖	↖
	BOB's detected bit values	1	1	0	1	1	1	0	0
Public discussion (i.e., sifting)	BOB tells ALICE the basis choices he made	Rect	Diag	Diag	Rect	Diag	Diag	Diag	Diag
	ALICE tells BOB which bits to keep		✓		✓		✓	✓	
	ALICE and BOB's shared sifted key	–	1	–	1	–	1	0	–

➠ QUANTUM KEY DISTRIBUTION



QUANTUM KEY DISTRIBUTION

Problemas en QKD

```
char *mail_auth(char *mechanism, authresponse_t resp, int argc, char *argv[])
{
    char tmp[MAILTMPLEN];
    AUTHENTICATOR *auth;
                                /* make upper case copy of mechanism name */
    ucase(strcpy(tmp, mechanism));
    for(auth = mailauthenticators; auth; auth = auth->next)
        if(auth->server && !strcmp(auth->name, tmp))
            return (*auth->server) (resp, argc, argv);
    return NIL;     /* no authenticator found */
}
```

➡ QUANTUM KEY DISTRIBUTION

Problemas en QKD

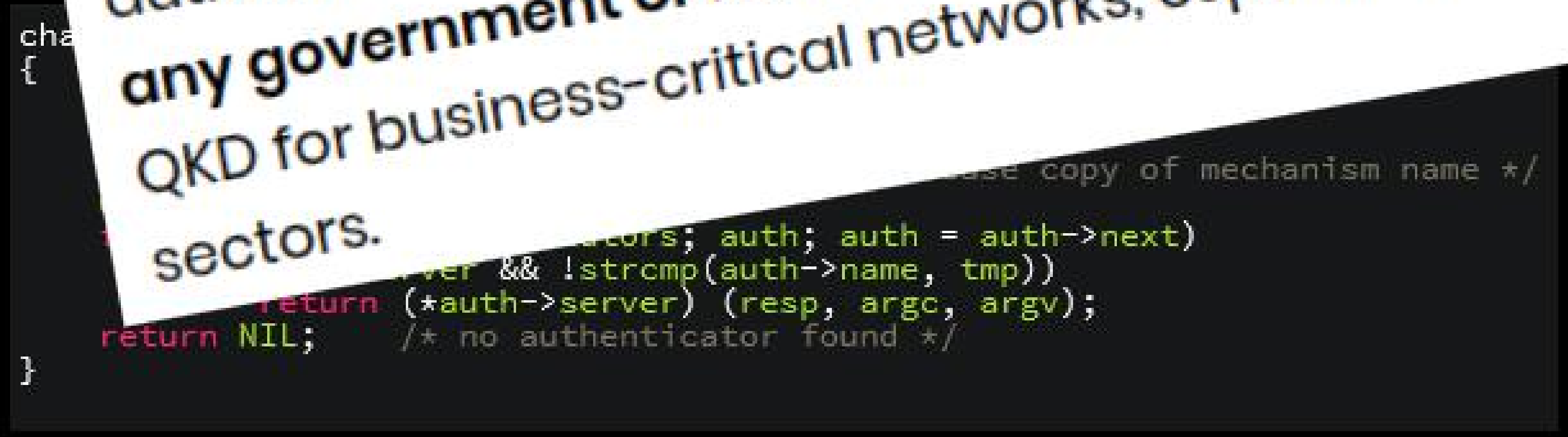
```
char *mail_auth(char *mechanism, authresponse_t resp, int argc, char *argv[])
{
    char tmp[MAILTMPLEN];
    AUTHENTICATOR *auth;
                                /* make upper case copy of mechanism name */
    ucase(strcpy(tmp, mechanism));
    for(auth = mailauthenticators; auth; auth = auth->next)
        if(auth->server && !strcmp(auth->name, tmp))
            return (*auth->server) (resp, argc, argv);
    return NIL;     /* no authenticator found */
}
```

➡ QUANTUM KEY DISTRIBUTION

Problemas en QKD

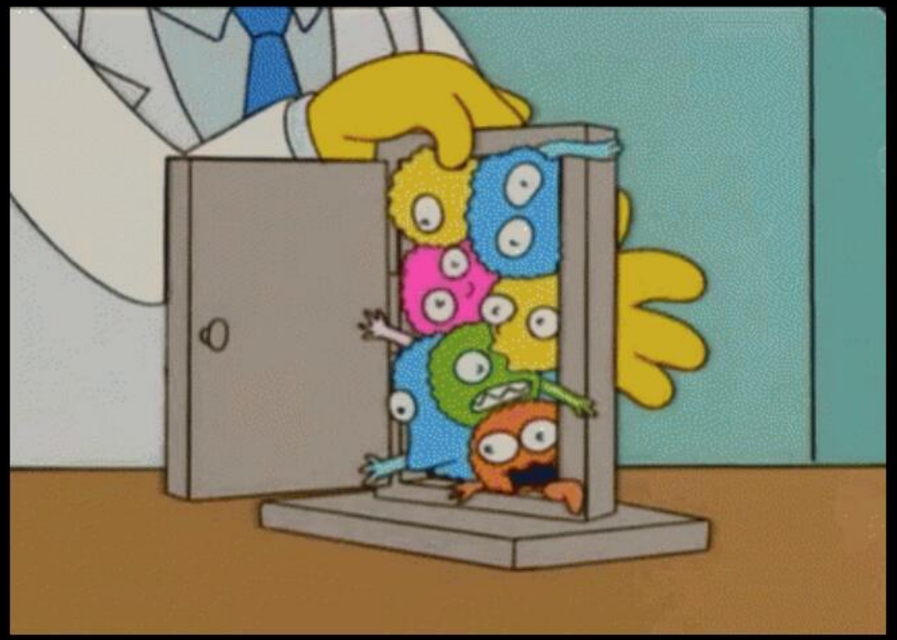
NCSC Position

Given the specialised hardware requirements of QKD over classical cryptographic key agreement mechanisms and the requirement for authentication in all use cases, the **NCSC does not endorse the use of QKD for any government or military applications**, and cautions against sole reliance on QKD for business-critical networks, especially in Critical National Infrastructure sectors.



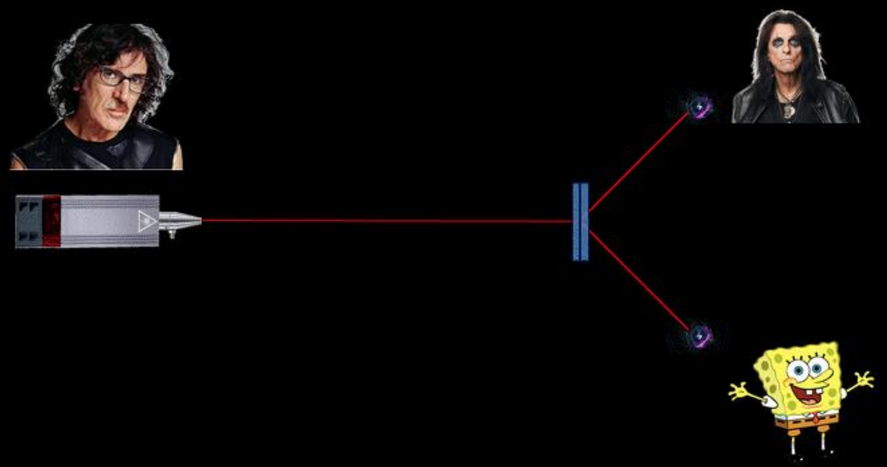
QUANTUM KEY DISTRIBUTION

COMUNICACION CUANTICA



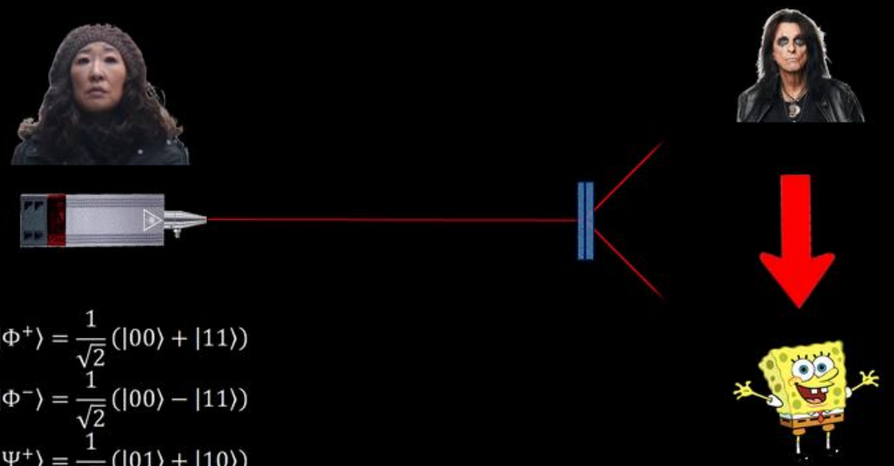
➠SUPER - DENSE CODING

Transmitir 2 bits clásicos con 1 qubit.



➠SUPER -DENSE CODING

Transmitir 2 bits clásicos con 1 qubit.

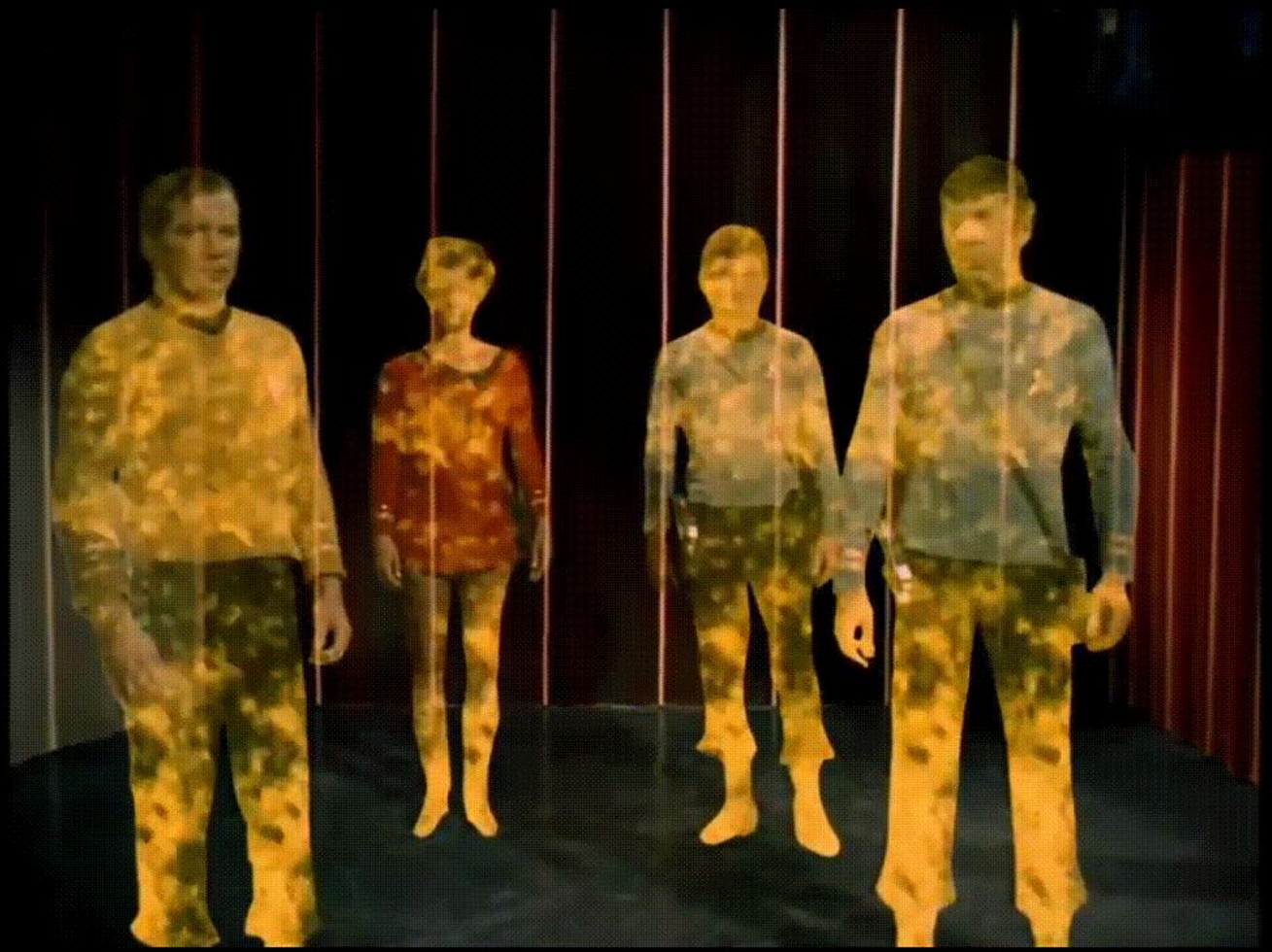


$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

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	$-\|10\rangle + \|01\rangle$

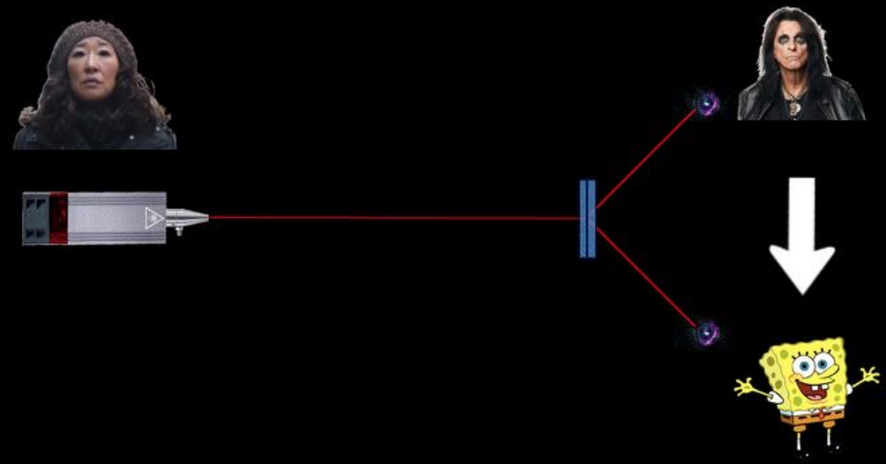
Bob Receives ($\cdot\frac{1}{\sqrt{2}}$)	After CNOT-gate ($\cdot\frac{1}{\sqrt{2}}$)	After H-gate
$\|00\rangle + \|11\rangle$	$\|00\rangle + \|10\rangle$	$\|00\rangle$
$\|10\rangle + \|01\rangle$	$\|11\rangle + \|01\rangle$	$\|01\rangle$
$\|00\rangle - \|11\rangle$	$\|00\rangle - \|10\rangle$	$\|10\rangle$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

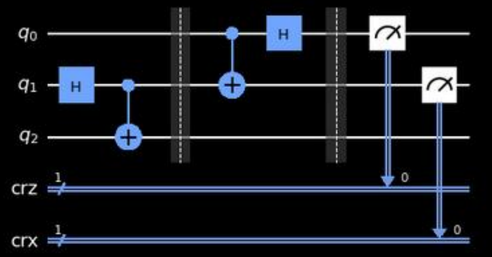
➠SUPER - DENSE CODING



TELEPORTATION

Transmitir 1 qubit, usando 2 bits clásicos.





00 → Do nothing

01 → Apply X gate

10 → Apply Z gate

11 → Apply ZX gate

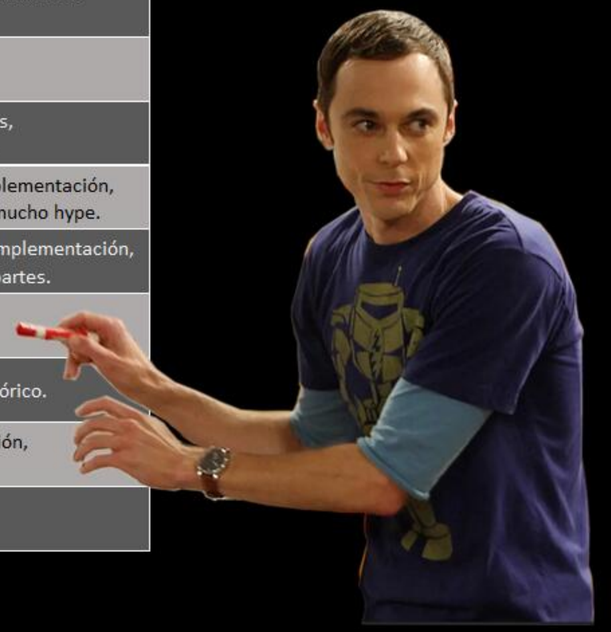
TELEPORTATION

Hey Bob! please check...

➠SUPERLUMINIC COMMUNICATION

RESUMEN

	Técnica	Funciones	Mejora	Madurez	Problemas/Vulnerabilidades
Computación cuántica	Shor	Romper RSA, QFT.	+++++	+	Hacerlo andar.
	Grover	Romper AES, Búsqueda en BD.	++	++	Hacerlo andar.
	QNN	Correr NN en computadoras cuánticas.	-	++	Muy poca mejora respecto a NN clásicas.
	QKM	Clasificar más rápido.	++	++	Adversary attacks.
Criptografía cuántica	PQC	Prepararse para cuando llegue Shor.	(+++++)	+	Algoritmos no probados, implementación, hype.
	QRNG	"True random" number generators.	++	--	Bias!, black boxes, implementación, side channel attacks, mucho hype.
	QKD	Distribuir claves en forma segura.	++	+++	Muy caro, muy lento, implementación, DoS, no autentica las partes.
Comunicación cuántica	Superdense Coding	Transmisión segura, codificar 2 bits en 1 qubit.	+++	--	Todavía teórico.
	Teleportation	Transmisión segura, qubit state.	+++	--	Muy baja velocidad, teórico.
	Memoria cuántica	Almacenar estados cuánticos, reducir espacio físico.	++++	----	Poco tiempo de retención, límite de distancia.
	Repetidores	Alcanzar mayores distancias.	+	--	MITM!!!



EKOPARTY

MUCHAS GRACIAS !!!

Carlos Benitez
@ch4r1i3b
carlos<at>platinumciber.com
https://cybersonthestorm.com
https://github.com/ch4r1i3b

Not only does God play dice, but... he sometimes throws them where they cannot be seen. (Stephen Hawking)

REFERENCIAS

Curso Linux Foundation WEF
https://trainingportal.linuxfoundation.org/learn/course/fundamentals-of-quantum-computing-lfq101/

Grover's Algorythm
http://twistedoakstudios.com/blog/Post2644_grovers-quantum-search-algorithm

Malware detection QML
https://github.com/D3Rkness/Malware-Detection-A-Quantum-Machine-Learning-Approach

QSVM
https://arxiv.org/pdf/1804.11326.pdf

Superdense Coding
https://qexperiments.blogspot.com/2020/07/quantum-malware-hacking-quantum-dense.html

Post Quantum NIST
https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/faqs
https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions

Vulnerabilidades en QRNG
https://eprint.iacr.org/2017/842.pdf
https://www.youtube.com/watch?v=UR5Tb8VtQds

Vulnerabilidades en QKD
https://iopscience.iop.org/article/10.1088/1367-2630/aade06
https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/
https://www.nature.com/articles/nphoton.2010.214
https://journals.aps.org/pra/abstract/10.1103/PhysRevA.87.062329
https://www.idquantique.com/quantum-safe-security/quantum-key-distribution/
https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies

Labs IBM Quantum
https://lab.quantum-computing.ibm.com/
https://quantum-computing.ibm.com/composer

Richard Feynman hablando de cuántica
https://www.youtube.com/watch?v=xdZMXWmlp9g