



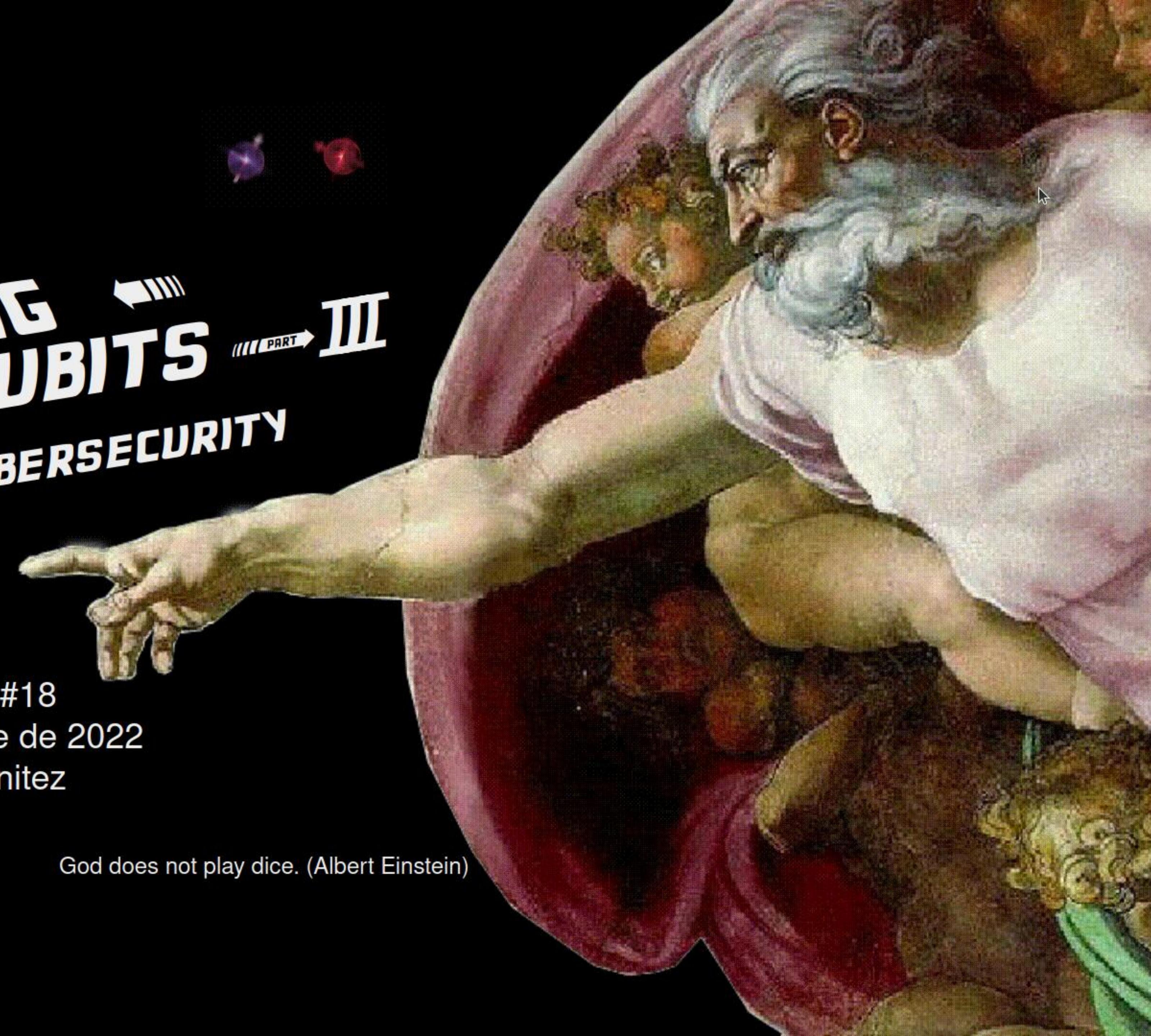
# PLAYING WITH QUBITS

Quantum Cybersecurity

Part III

Ekoparty #18  
2 de Noviembre de 2022  
Carlos Benitez

God does not play dice. (Albert Einstein)





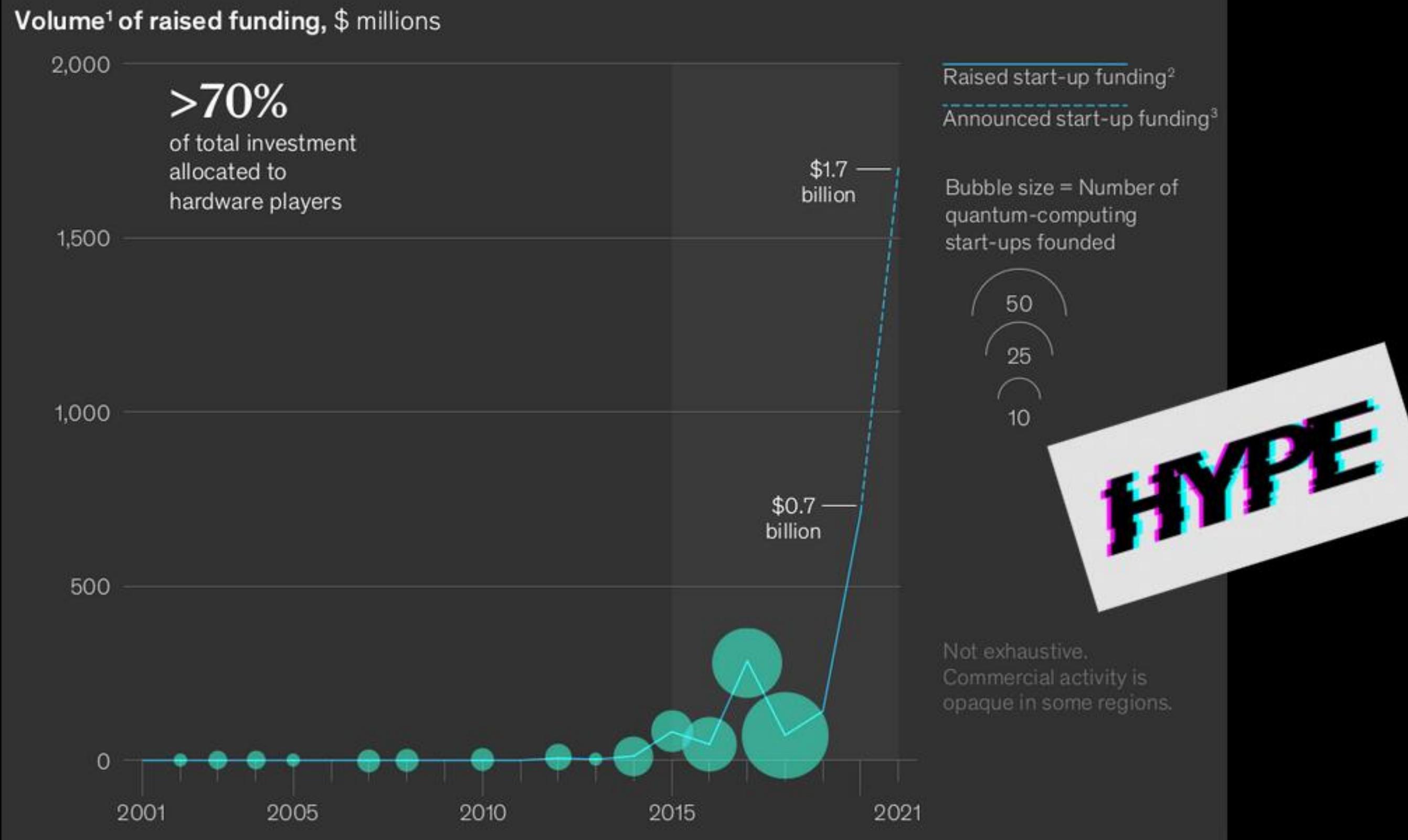
## Carlos Benitez

- 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?



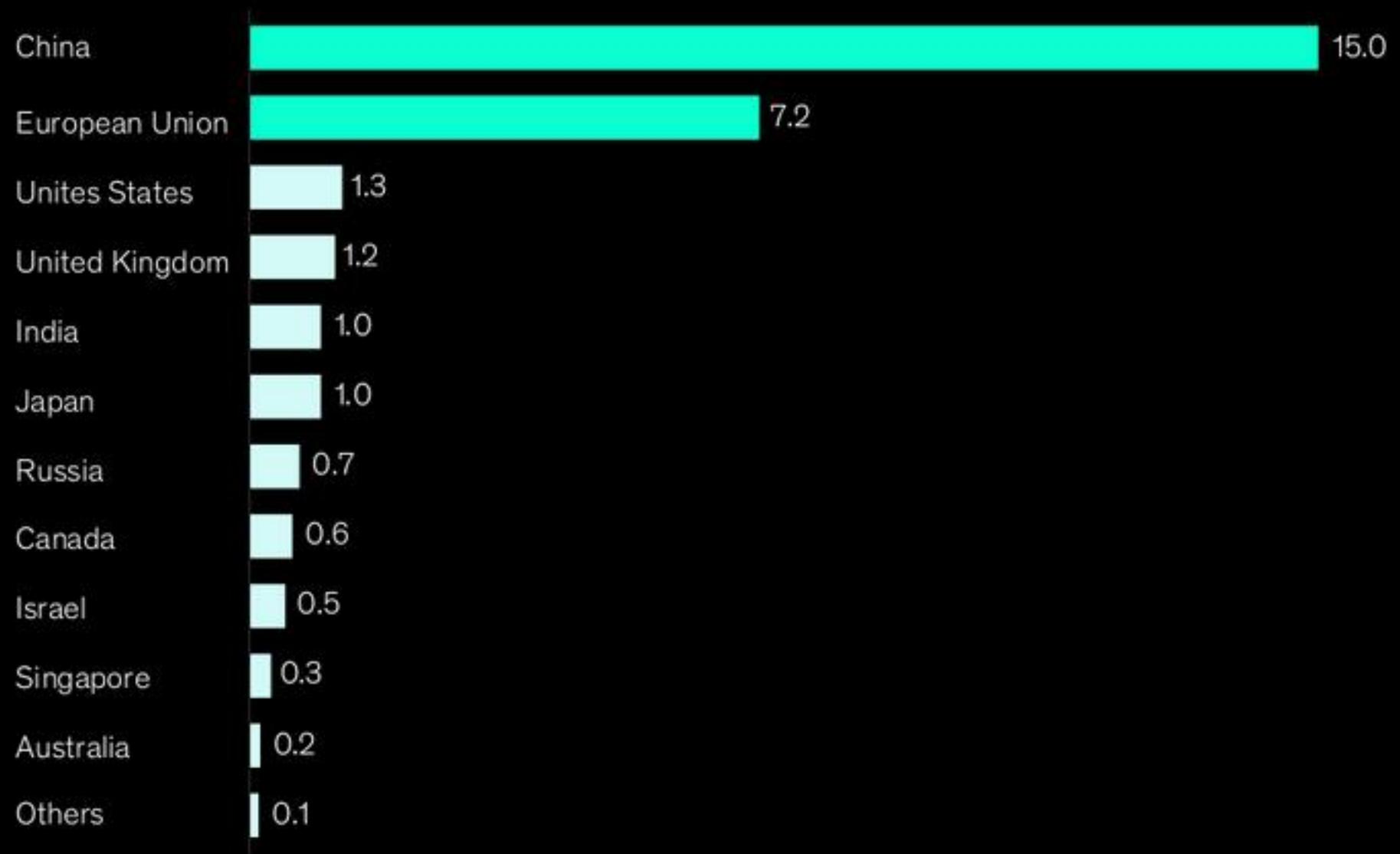
Start-up activity and investments in quantum computing have skyrocketed since 2015.



**HABLEMOS DE NUMEROS**

**China and the European Union lead significantly on public funding for quantum computing.**

Announced planned governmental funding,<sup>1</sup> \$ billions



EU public funding sources, %



**HABLEMOS DE NUMEROS**

**EKOPARTY**

Luciano Bello

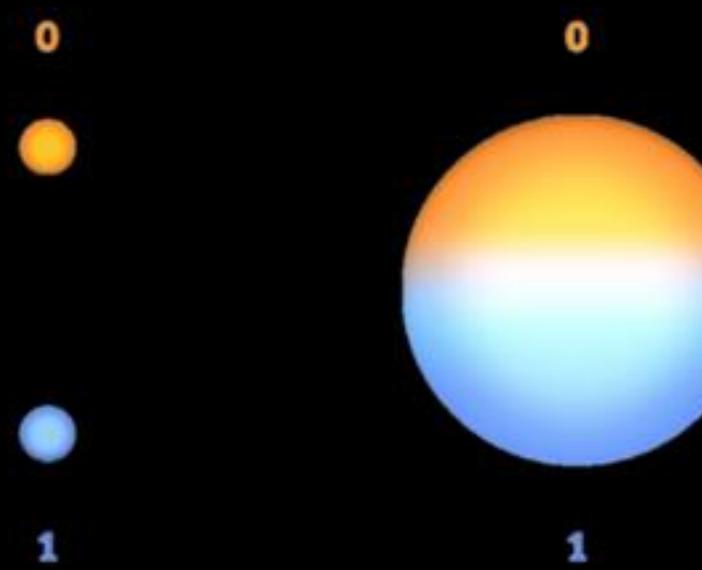
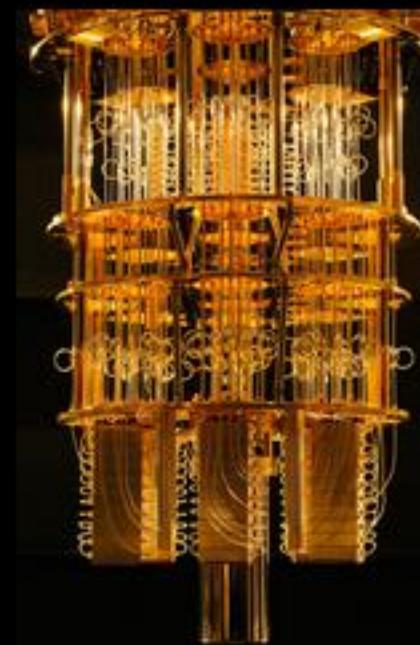
Fernando Virdia

***AGRADECIMIENTOS***

A  
PREVIOUSLY

# ► PLAYING WITH QUBITS I

## ► CONCEPTOS COMPUTACION CUANTICA

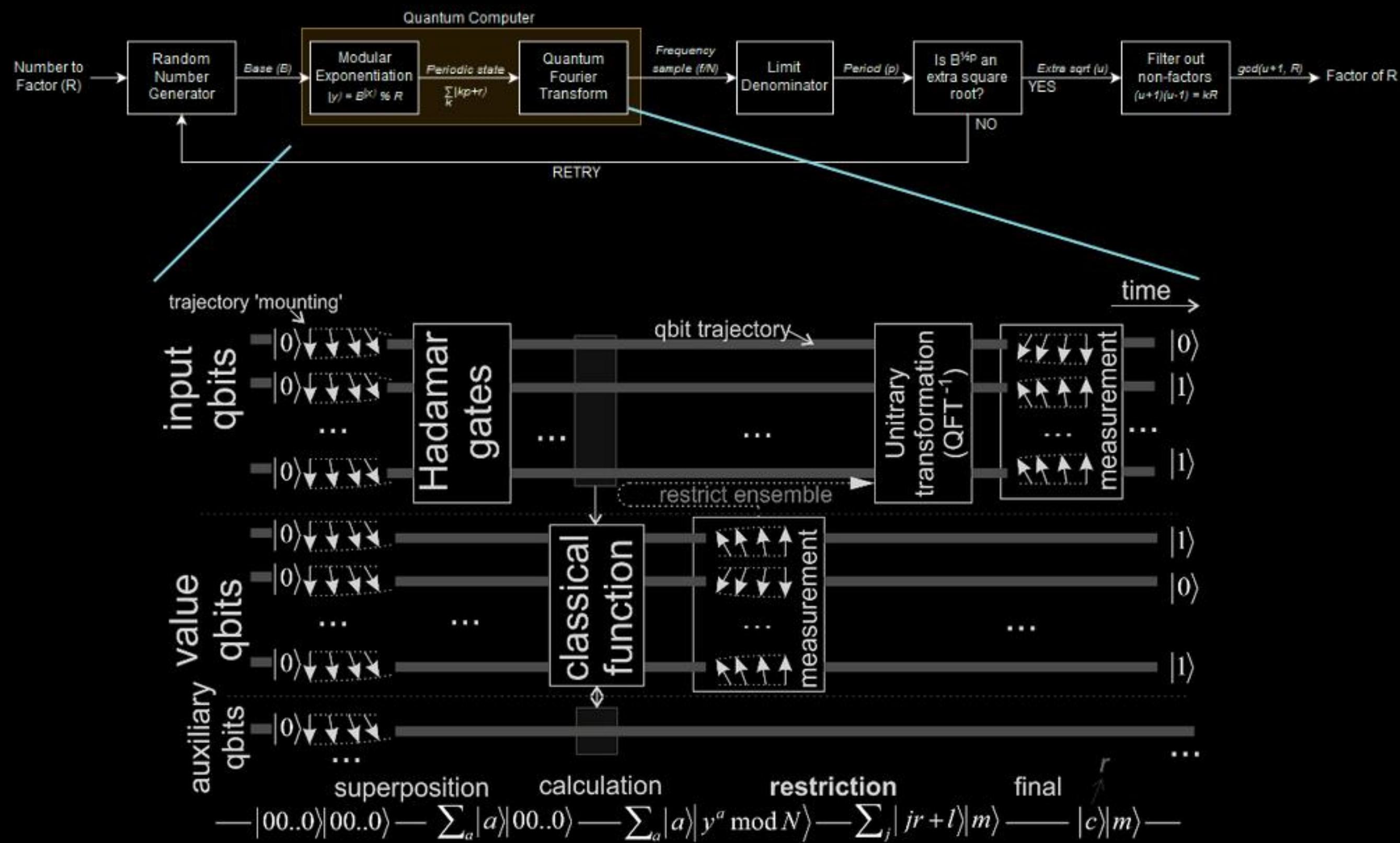


$x$	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$
0	0	1	1	0
1	1	0	1	0

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

# ► PLAYING WITH QUBITS !!

## ► EL ALGORITIMO DE SHOR



## »»» PLAYING WITH QUBITS    |||



- CONCEPTOS
- COMPUTACION CUANTICA
- CRIPTOGRAFIA POST-CUANTICA
- CRIPTOGRAFIA CUANTICA
- COMUNICACION CUANTICA
- RESUMEN

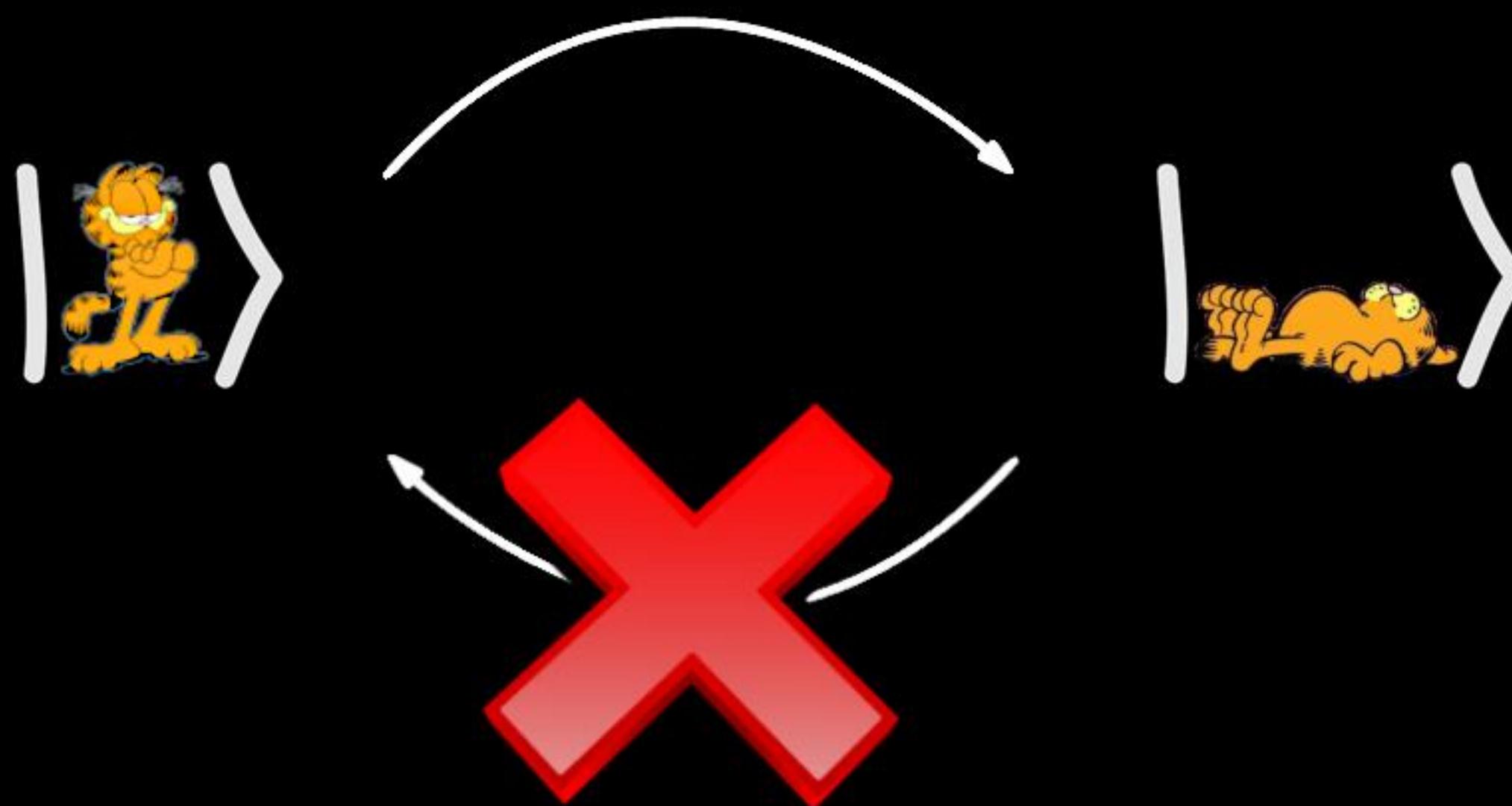


► CONCEPTOS



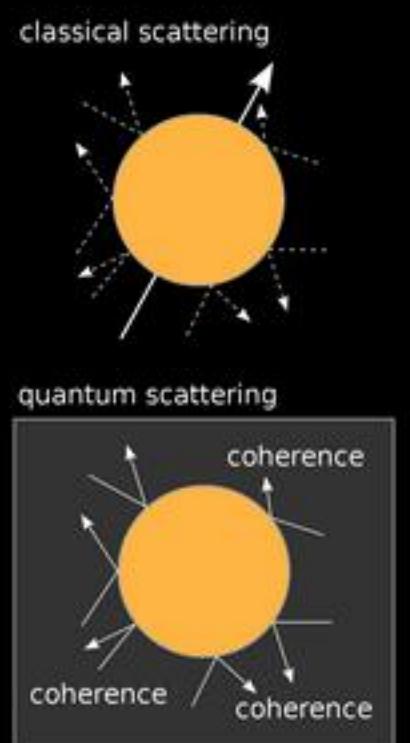
➡SUPERPOSICION

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

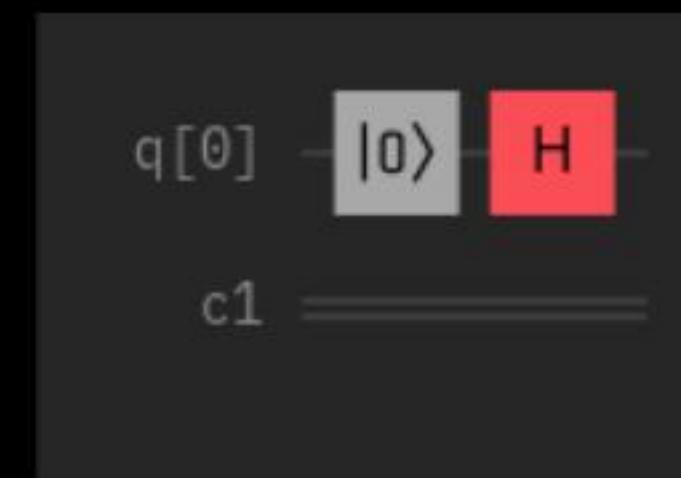


➡ SUPERPOSICION

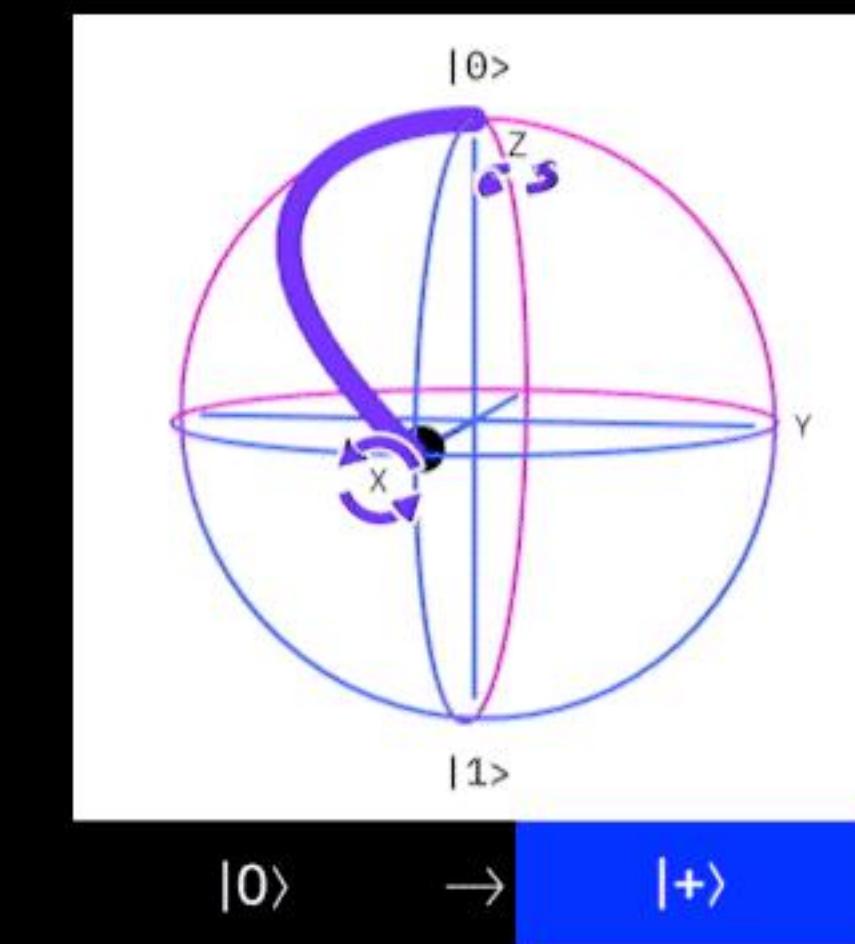
$$\frac{1}{\sqrt{2}}| \text{Garfield} \rangle + \frac{1}{\sqrt{2}}| \text{asleep Garfield} \rangle$$



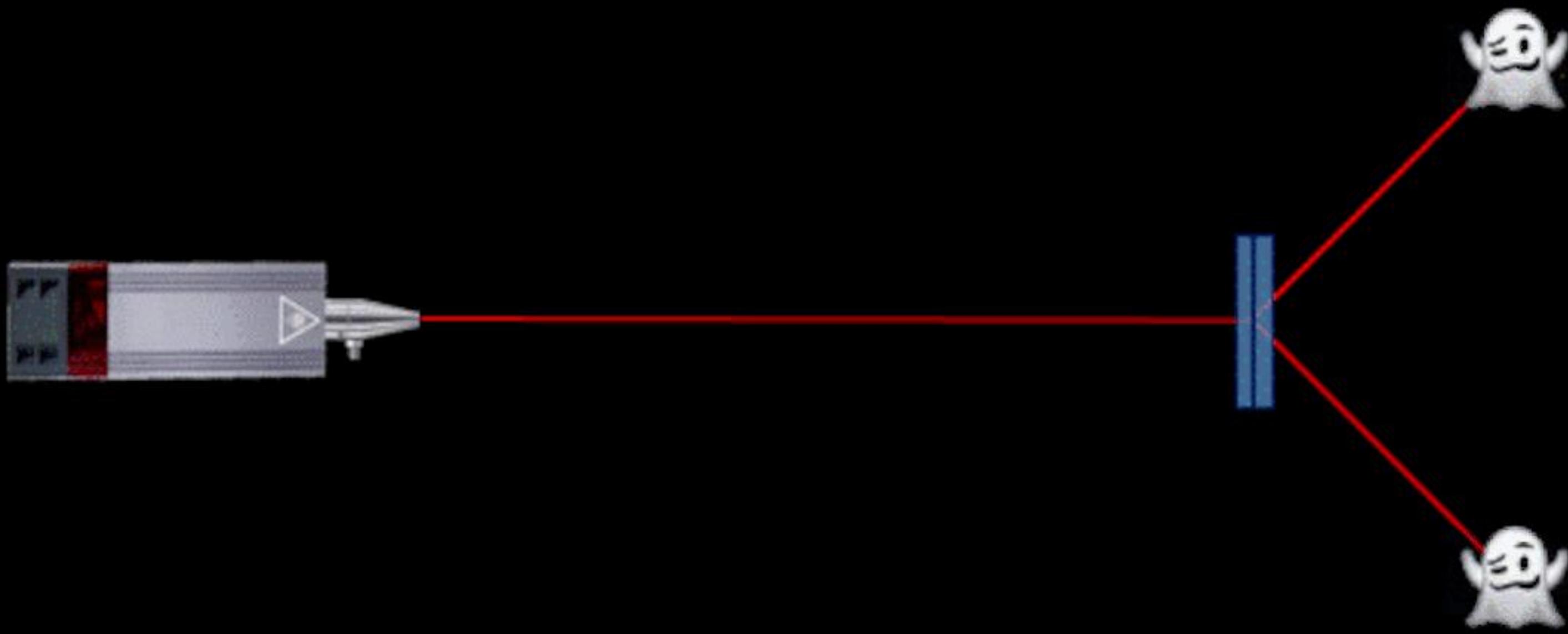
➡SUPERPOSICION



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



➡ SUPERPOSICION



➡ ENTANGLEMENT



➡ 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)

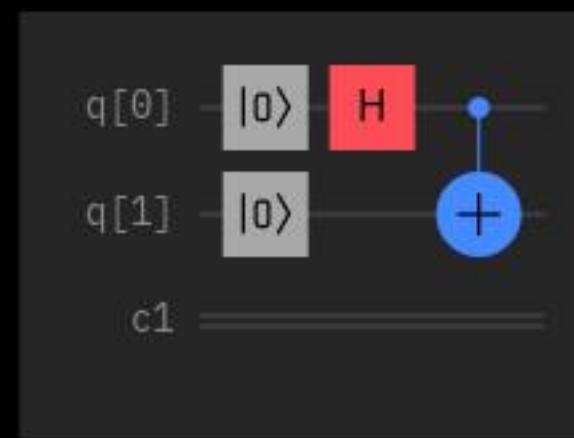
### I. Introduction

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 non-local structure. This is characteristic, according to the result to be proved here, of any such theory which reproduces exactly the quantum mechanical predictions.

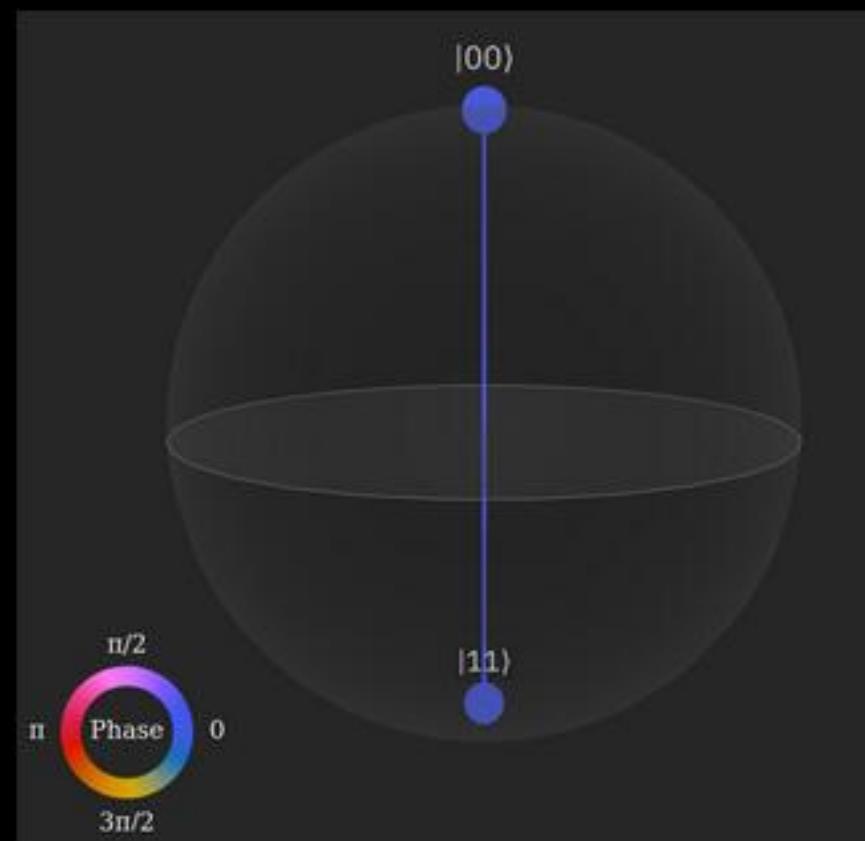
### II. Formulation

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

➡ ENTANGLEMENT



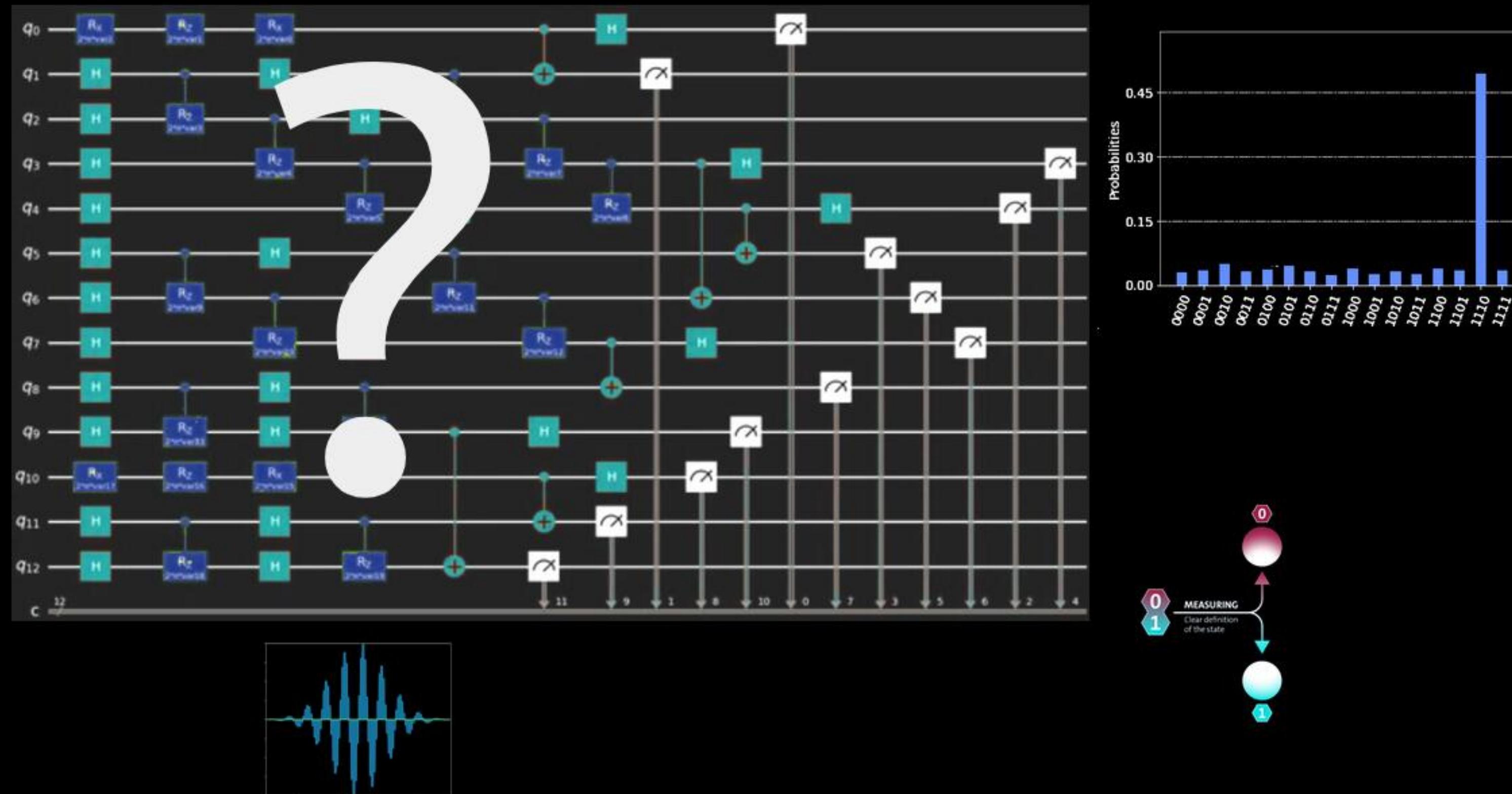
$$H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad \text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

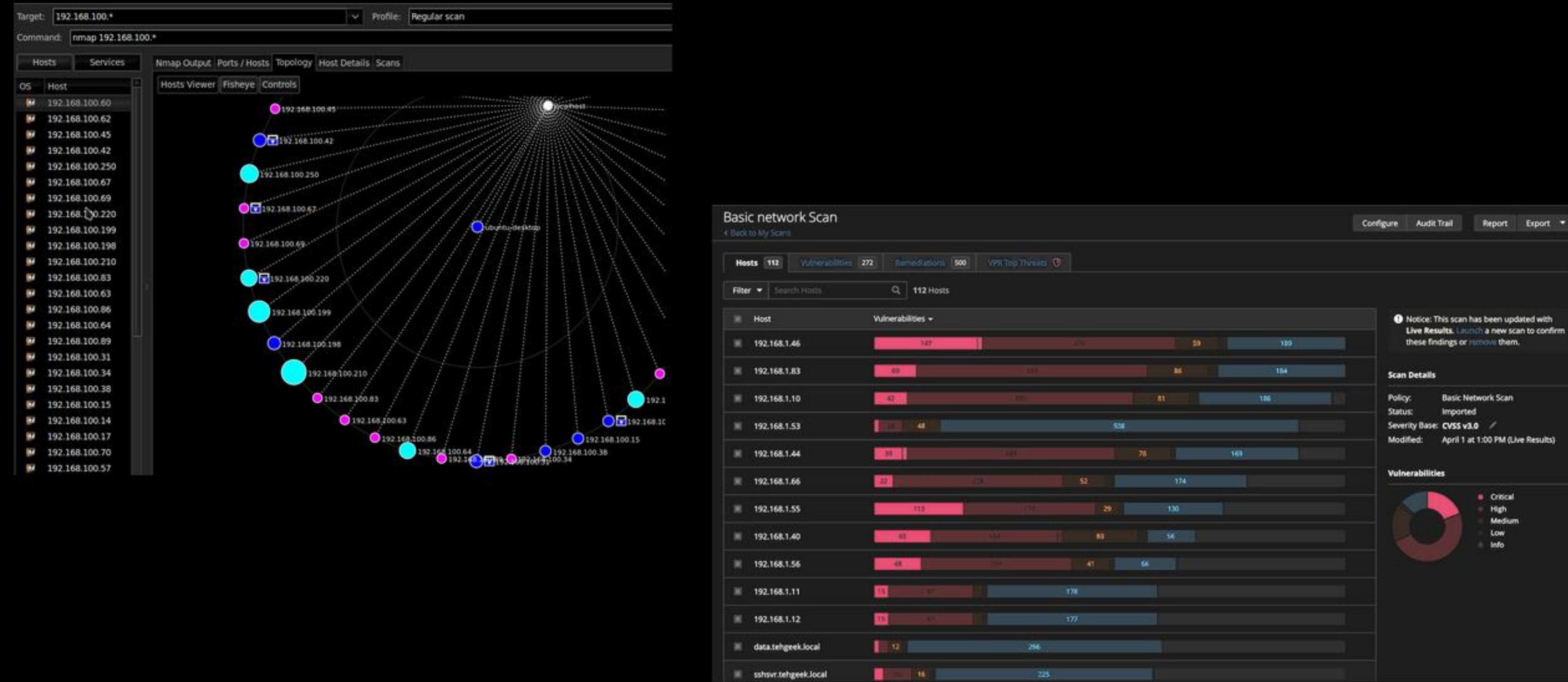


➡ ENTANGLEMENT



# » COMPUTACION CUANTICA





» LD QUE NO SE PUEDE HACER

Quantum Cyphyr Platforms

The screenshot shows a web-based penetration testing tool. At the top left is a logo featuring a stylized dragon-like creature inside a triangle with the words "Quantum" and "Cyphyr". To the right of the logo is a navigation bar with links: WELCOME, WHY QCP, COMPANY, SERVICES (which is highlighted in blue), RESOURCE PORTAL, CAREER PORTAL, and CONTACT PORTAL. Below the navigation bar is a large yellow section containing the heading "Quantum Penetration Testing". Underneath this heading is a paragraph of text: "WITH PROVEN QUANTUM PENETRATION TESTING METHODOLOGIES AND STATE-OF-THE-ART SECURITY TOOLS WE PROVIDE YOU WITH THE INFORMATION NECESSARY TO MITIGATE AND REMEDY YOUR SYSTEM AND NETWORK VULNERABILITIES." Below this text is a quote: "WHAT DOES MY ORGANIZATION WANT OUT OF A PENETRATION TEST AND WHY?" and a descriptive paragraph: "A QUANTUM PENETRATION TEST (QPT) DOESN'T STOP AT SIMPLY UNCOVERING VULNERABILITIES: IT GOES THE NEXT STEP TO ACTIVELY EXPLOIT THOSE VULNERABILITIES IN ORDER TO PROVE (OR DISPROVE) REAL-WORLD ATTACK VECTORS AGAINST AN ORGANIZATION'S IT ASSETS, DATA, HUMANS, AND/OR PHYSICAL SECURITY." On the far left, there is a sidebar with a "Targets" section showing a list of IP addresses from 192.168.100.60 to 192.168.100.70. On the far right, there is a sidebar with sections for "Report", "Export", "Network Scan", and a legend for vulnerability severity levels: Critical (red), High (orange), Medium (yellow), Low (light green), and Info (grey).

Quantum Penetration Testing

WITH PROVEN QUANTUM PENETRATION TESTING METHODOLOGIES AND STATE-OF-THE-ART SECURITY TOOLS WE PROVIDE YOU WITH THE INFORMATION NECESSARY TO MITIGATE AND REMEDY YOUR SYSTEM AND NETWORK VULNERABILITIES.

"WHAT DOES MY ORGANIZATION WANT OUT OF A PENETRATION TEST AND WHY?"

A QUANTUM PENETRATION TEST (QPT) DOESN'T STOP AT SIMPLY UNCOVERING VULNERABILITIES: IT GOES THE NEXT STEP TO ACTIVELY EXPLOIT THOSE VULNERABILITIES IN ORDER TO PROVE (OR DISPROVE) REAL-WORLD ATTACK VECTORS AGAINST AN ORGANIZATION'S IT ASSETS, DATA, HUMANS, AND/OR PHYSICAL SECURITY.

» LD QUE NO SE PUEDE HACER



<- Algoritmo de Shor

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



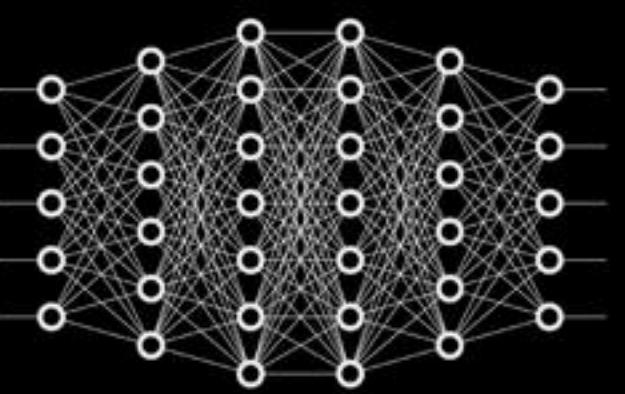
# AES

<- Algoritmo de Grover

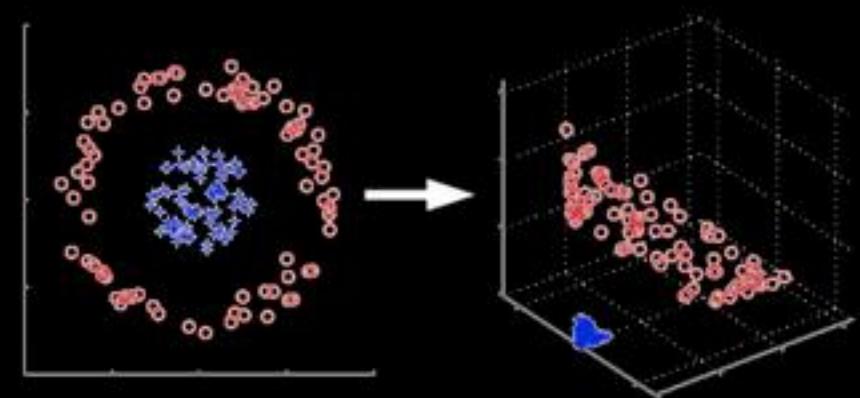
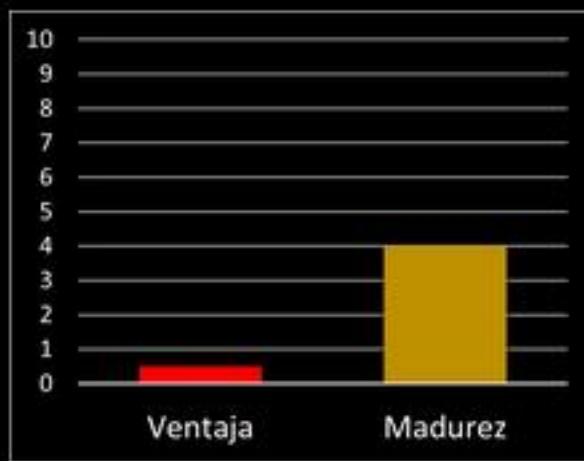
$$O(N) \rightarrow O(\sqrt{N})$$



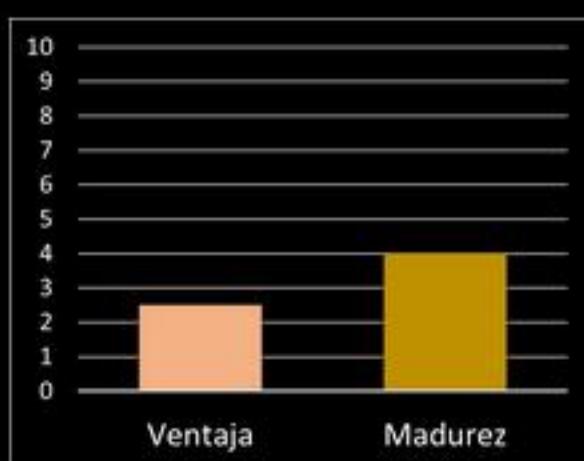
» LO QUE SI SE PUEDE HACER



<- QNN



<- QSVM/QKM



»»» LD QUE SI SE PUEDE HACER

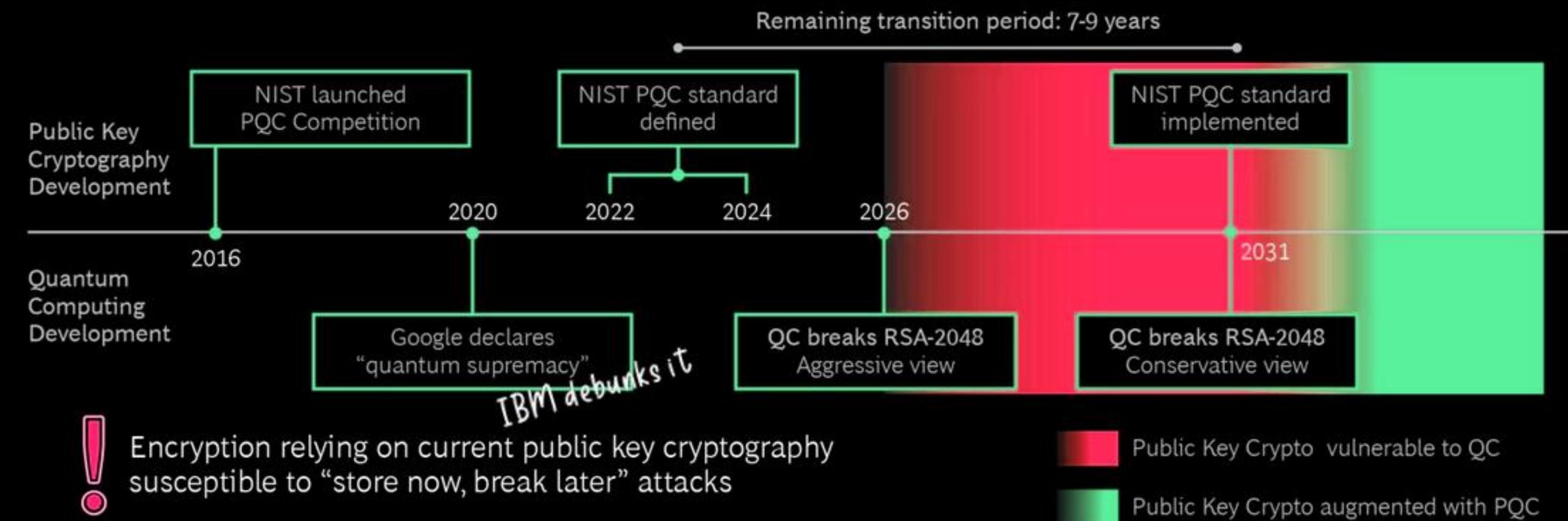
?

➡ LO QUE SE PODRIA HACER



## ➡ CRIPTOGRAFIA POST-CUANTICA

## Time Window for Upgrading Cryptographic Infrastructure

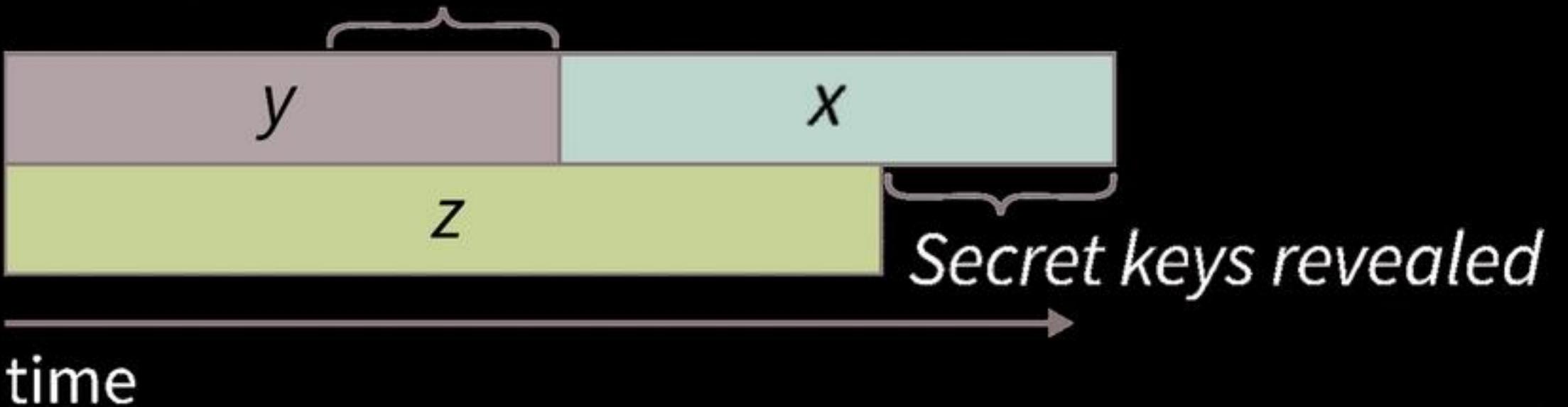


➡ LA AMENAZA POST-CUANTICA

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

Michele  
Mosca

What do we do here??



$x$  = período de seguridad de los datos

$y$  = período de transición a PQC

$z$  = tiempo para implementar Shor

➡ LA AMENAZA POST-CUANTICA

An official website of the United States government. Here's how you know:

**NIST**

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

Search CSRC  CSRC MENU

UPDATES 2022

## PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates

July 05, 2022

f t

### Summary

NIST has completed the third round of the Post-Quantum Cryptography (PQC) standardization process, which selects public-key cryptographic algorithms to protect information through the advent of quantum computers. A total of four candidate algorithms have been [selected for standardization](#), and four additional algorithms will continue into the [fourth round](#).

A detailed description of the decision process and selection rationale is included in NIST Internal Report (NIST IR) 8413, [Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process](#), which is also available on the [NIST PQC webpage](#). Questions may be directed to [pqc-comments@nist.gov](mailto:pqc-comments@nist.gov).

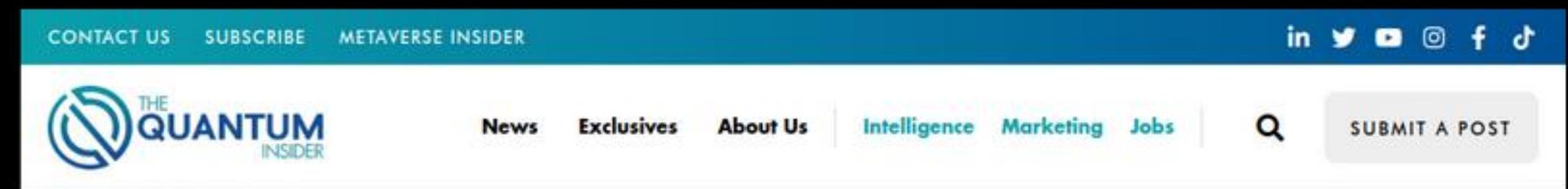
This announcement also discusses plans for a [Fourth PQC Conference](#) and an [upcoming call for additional quantum-resistant digital signature algorithms](#).

### PQC Fourth Round Candidate Key-Establishment Mechanisms (KEMs)

The following candidate KEM algorithms will advance to the fourth round:

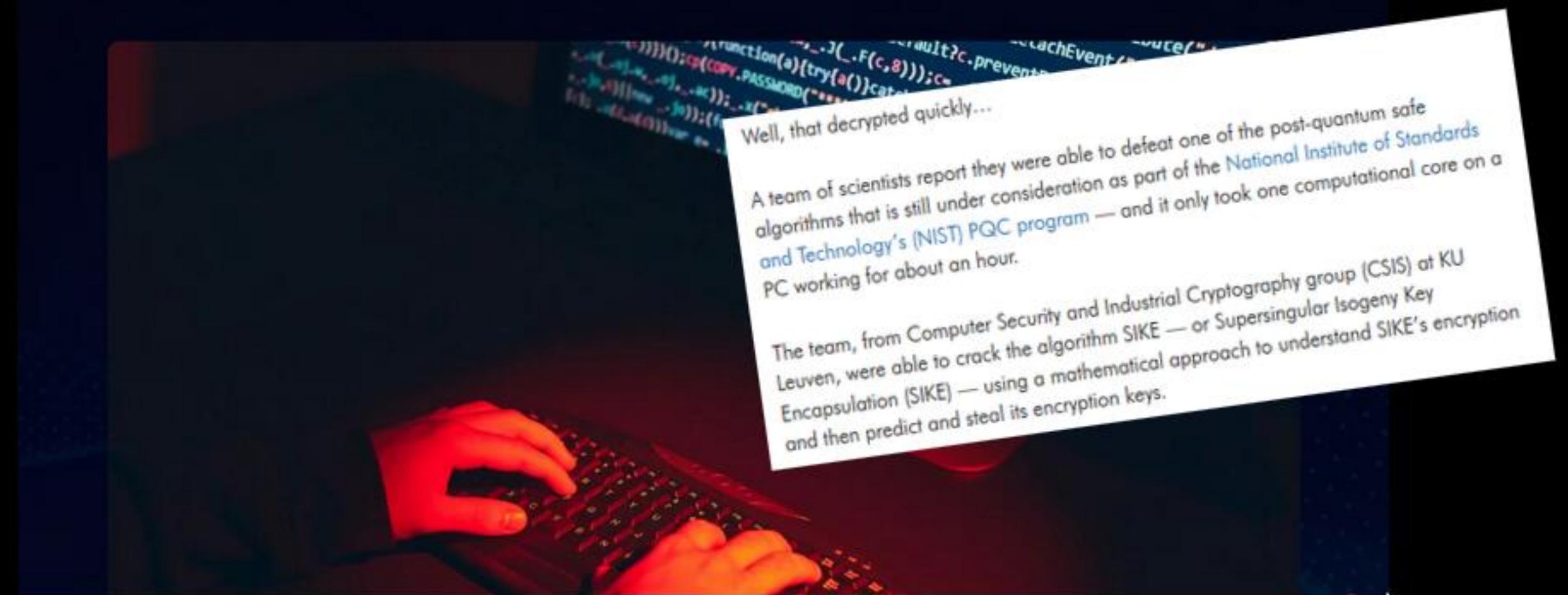
Public-Key Encryption/KEMs
BIKE
Classic McEliece
HQC
SIKE

➡ LA COMPETENCIA PQC NIST



# Post-Quantum Safe Algorithm Candidate Cracked in an Hour on a PC

BY MATT SWAYNE • AUGUST 5, 2022 • RESEARCH



Well, that decrypted quickly...  
A team of scientists report they were able to defeat one of the post-quantum safe algorithms that is still under consideration as part of the National Institute of Standards and Technology's (NIST) PQC program — and it only took one computational core on a PC working for about an hour.

The team, from Computer Security and Industrial Cryptography group (CSIS) at KU Leuven, were able to crack the algorithm SIKE — or Supersingular Isogeny Key Encapsulation (SIKE) — using a mathematical approach to understand SIKE's encryption and then predict and steal its encryption keys.

➡ LA COMPETENCIA PQC NIST

Quantum-grade security.  
For today's organizations.

At QuSecure, we know that protecting valuable data, is today. in-one software-based quantum computing solution. We implement and effortless transition from today's technologies, and emerging ones alike, we offer our clients a post-quantum secure solution, so they're ready for today. And tomorrow.

QuProtect Key Features

100% standards-based and compliant  
Including NIST compliant, providing trusted delivery of post-quantum resilience

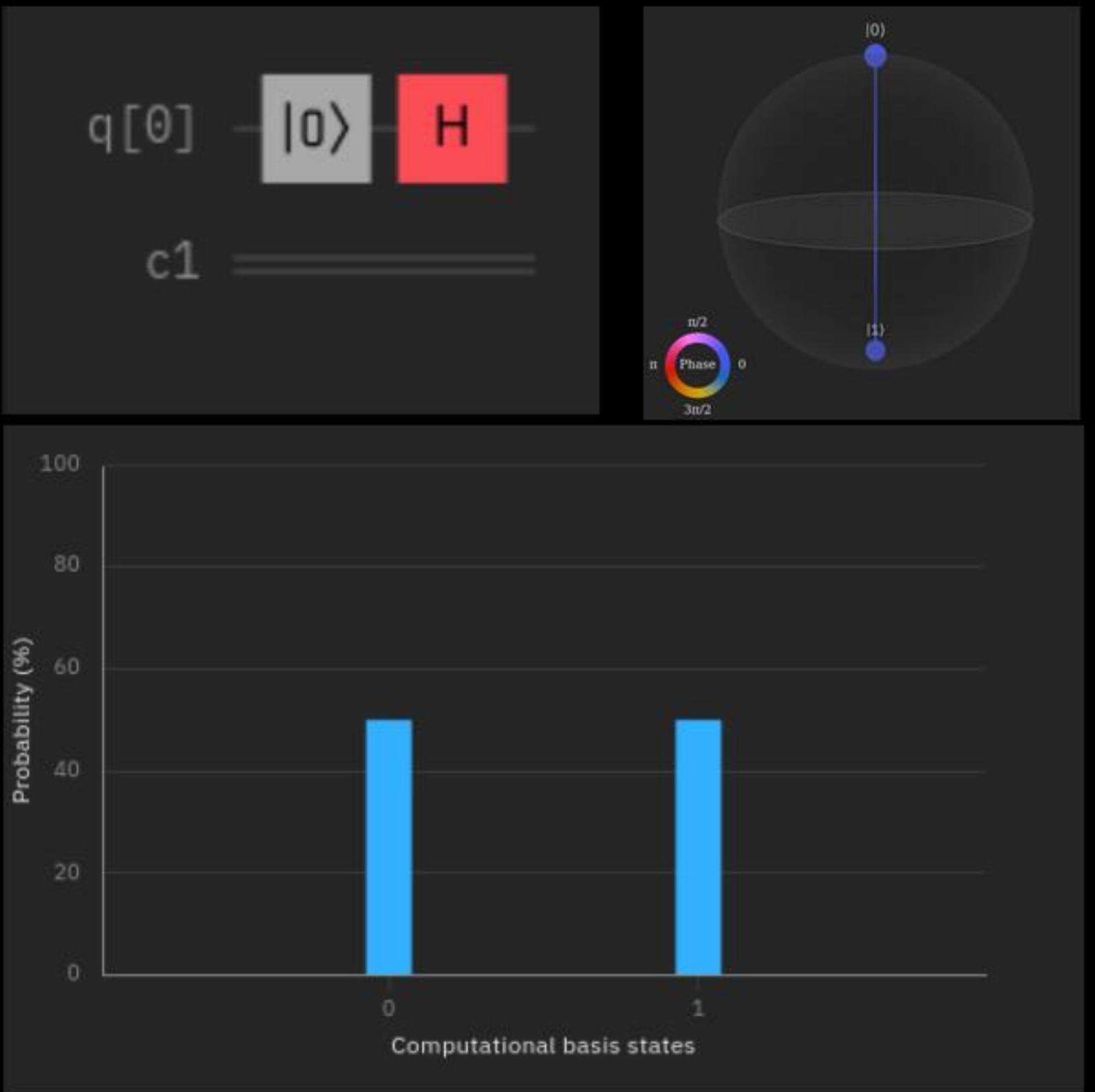
Find out more 

what???

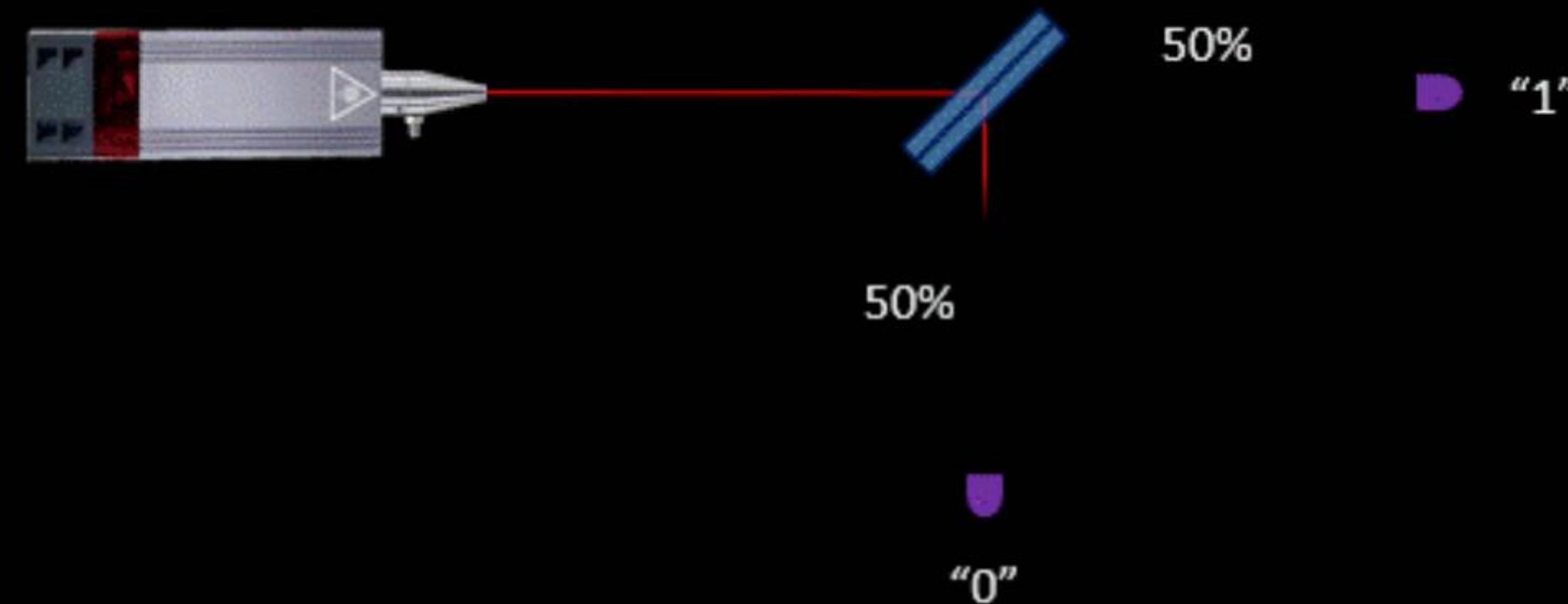
➡ LA AMENAZA POST-CUANTICA



# » CRIPTOGRAFIA CUANTICA



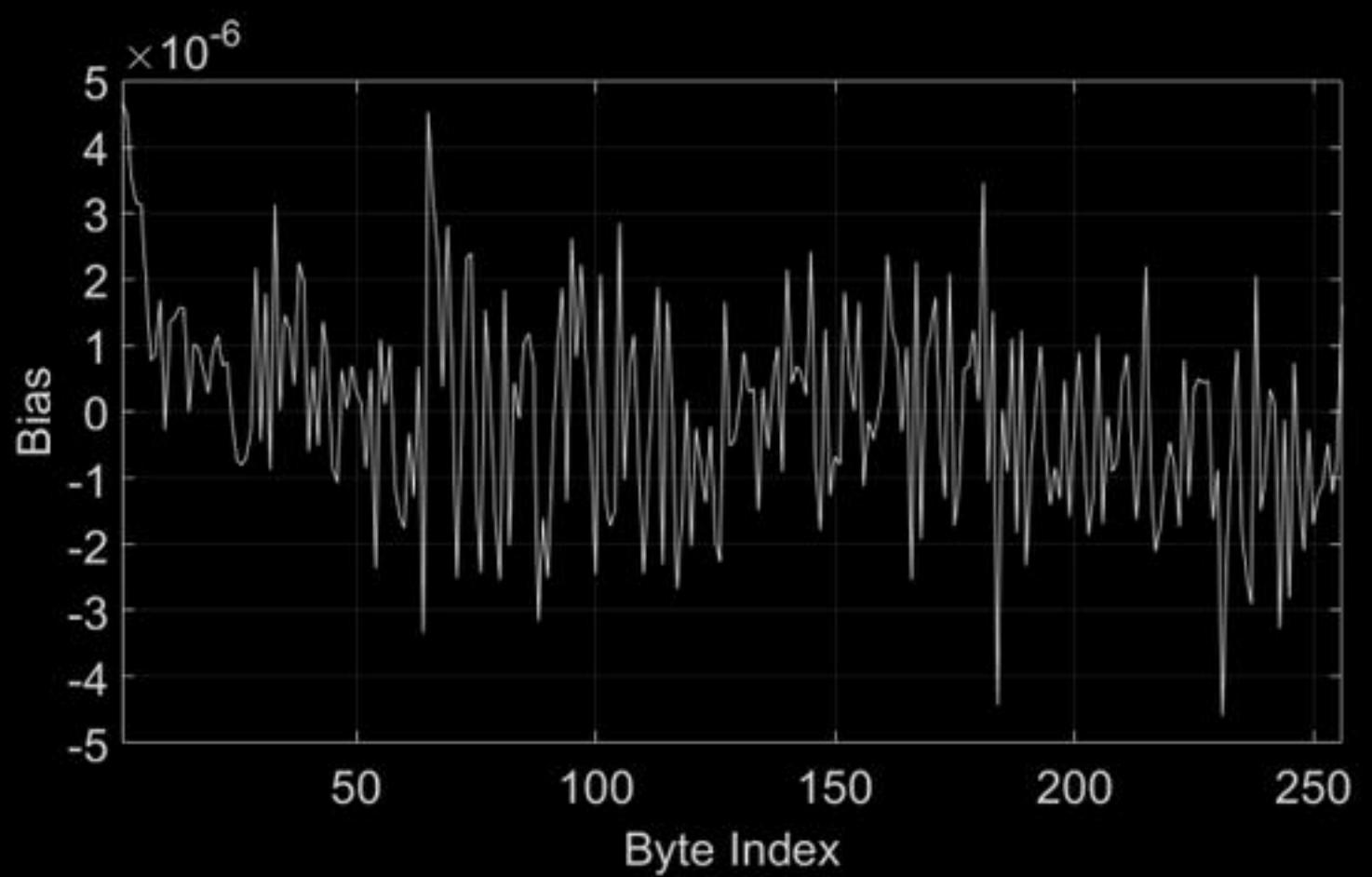
## ➡ QUANTUM RANDOM NUMBER GENERATION



## ➡ QUANTUM RANDOM NUMBER GENERATION



Bias!!



➡ QUANTUM RANDOM NUMBER GENERATION



➡ QUANTUM KEY DISTRIBUTION

# Classic public key cryptography



➡ QUANTUM KEY DISTRIBUTION



quantum generated keys  
quantum transmission channel

---

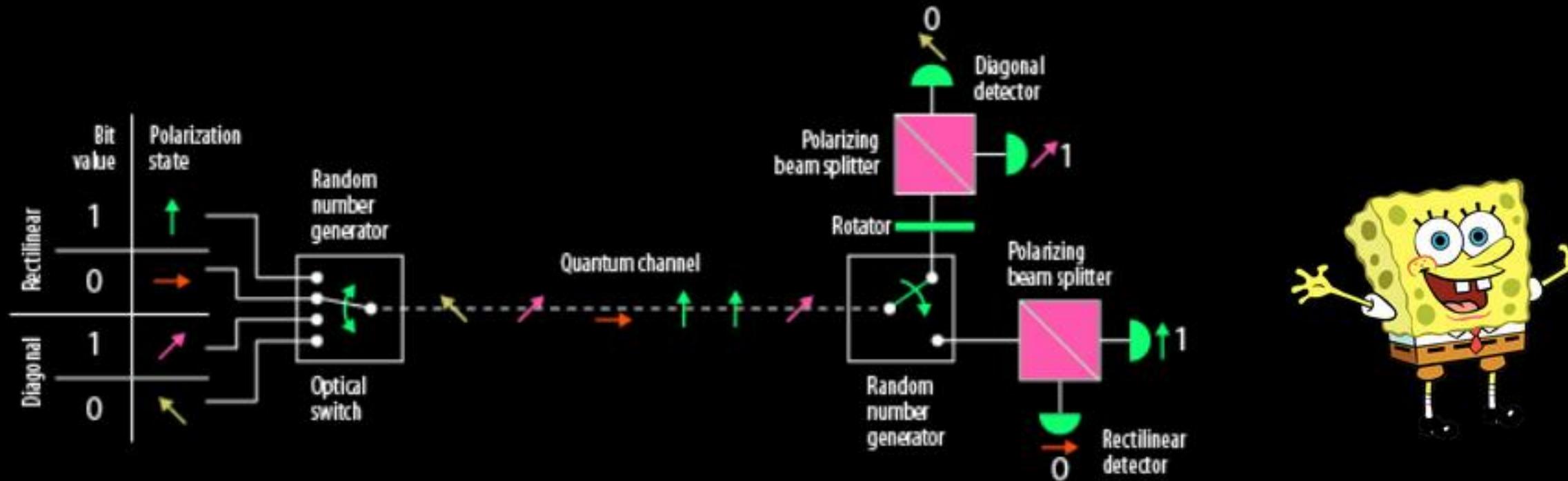
---



classic encrypted message  
classic transmission channel

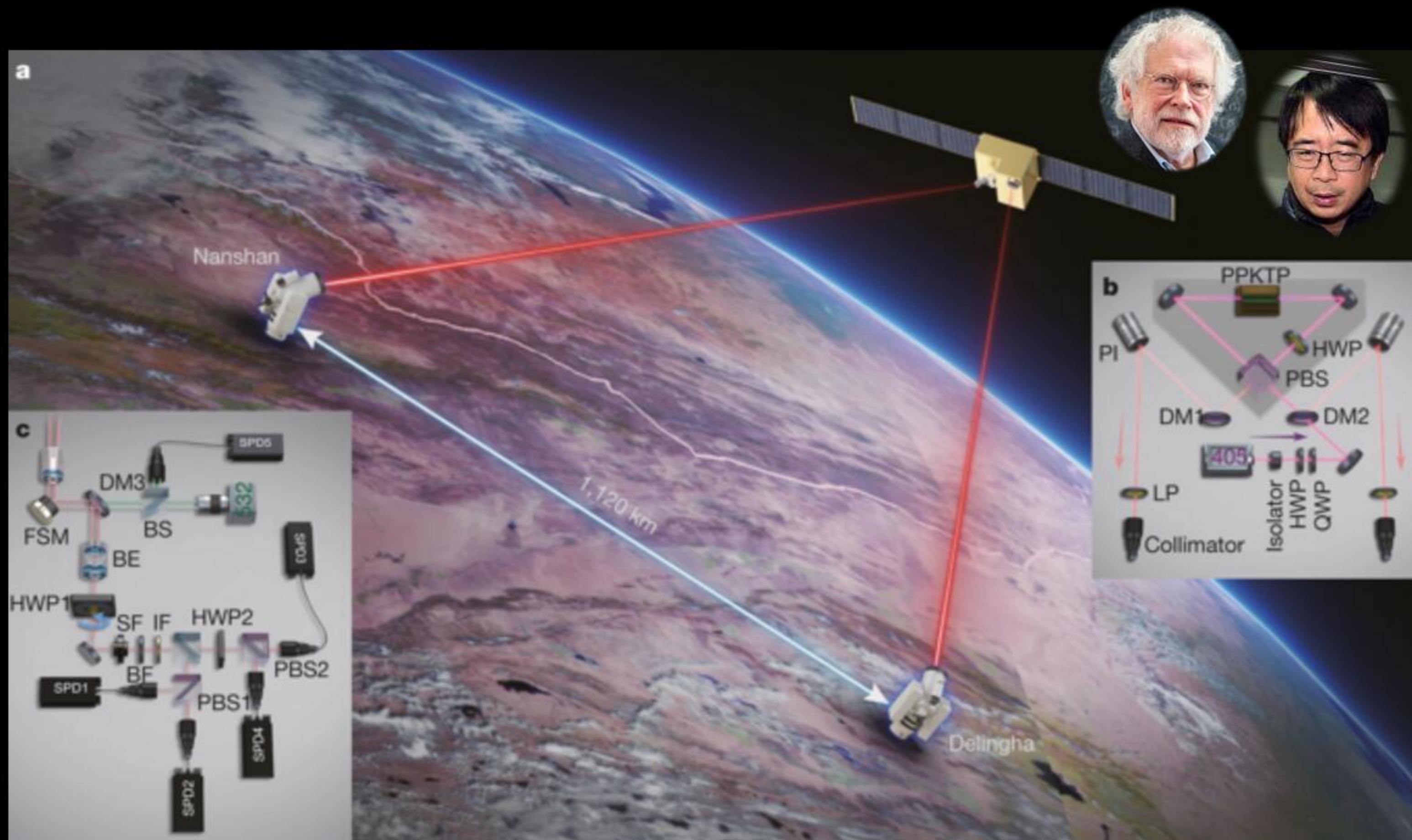
➡ QUANTUM KEY DISTRIBUTION

# BB84



	ALICE sends photons							
Quantum transmission& detection	0	1	0	1	1	1	0	1
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)	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(strncpy(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(strncpy(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**

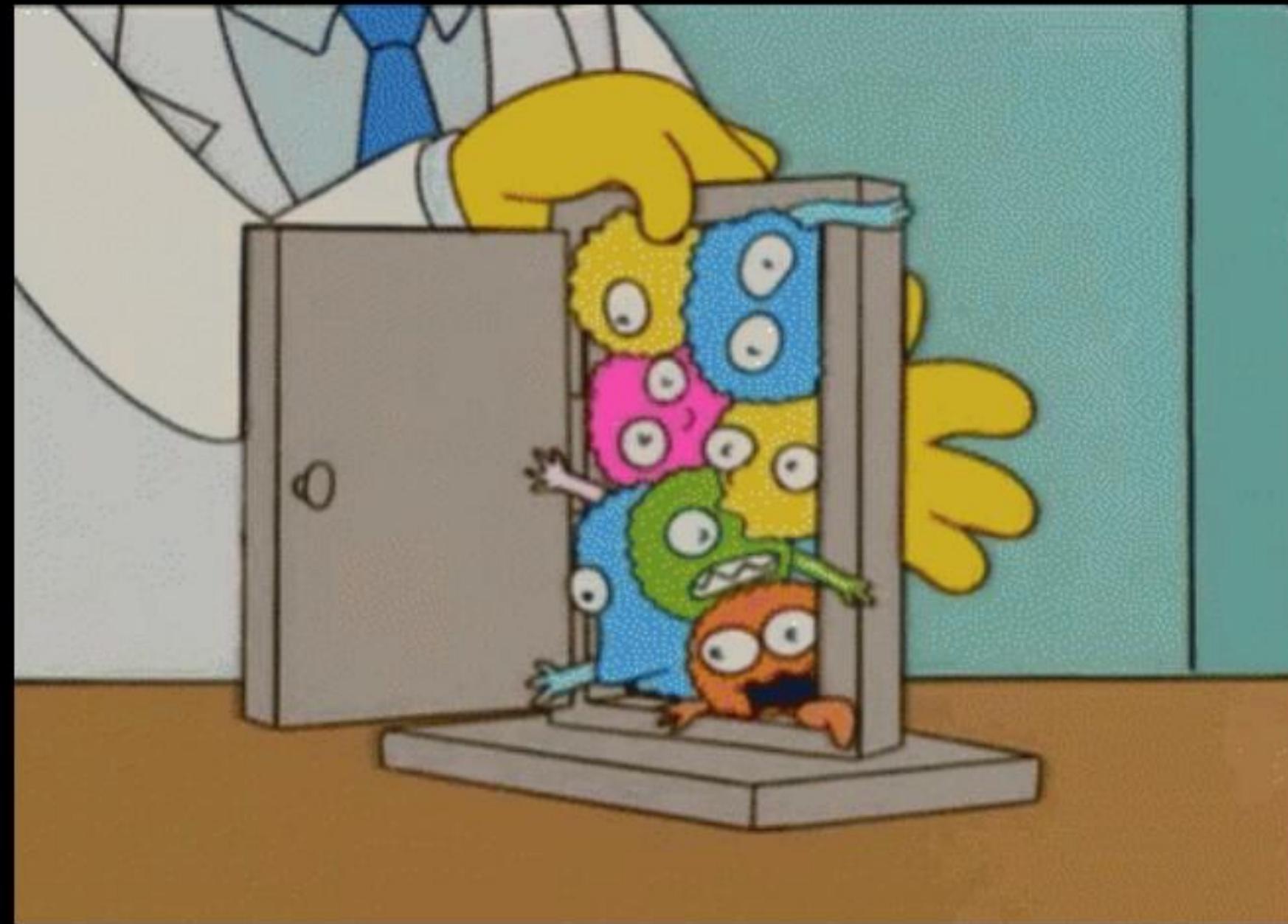
Given the specialised hardware requirements of QKD over classical cryptographic key agreement mechanisms and the requirement for authentication in all use cases, the NCSC does not endorse the use of QKD for any government or military applications, and cautions against sole reliance on QKD for business-critical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

```
char *getAuthenticatorByName(char *name) {  
    char *auth; /* pointer to authenticator */  
    /* ... */  
    /* loop through authenticators */  
    for (auth = authList; auth != NULL; auth = auth->next)  
        if (strcmp(auth->name, name) == 0) /* found */  
            /* copy of mechanism name */  
            /* ... */  
            /* return pointer to authenticator */  
            /* ... */  
            /* no authenticator found */  
            /* ... */  
    return NIL;  
}
```

➡ QUANTUM KEY DISTRIBUTION

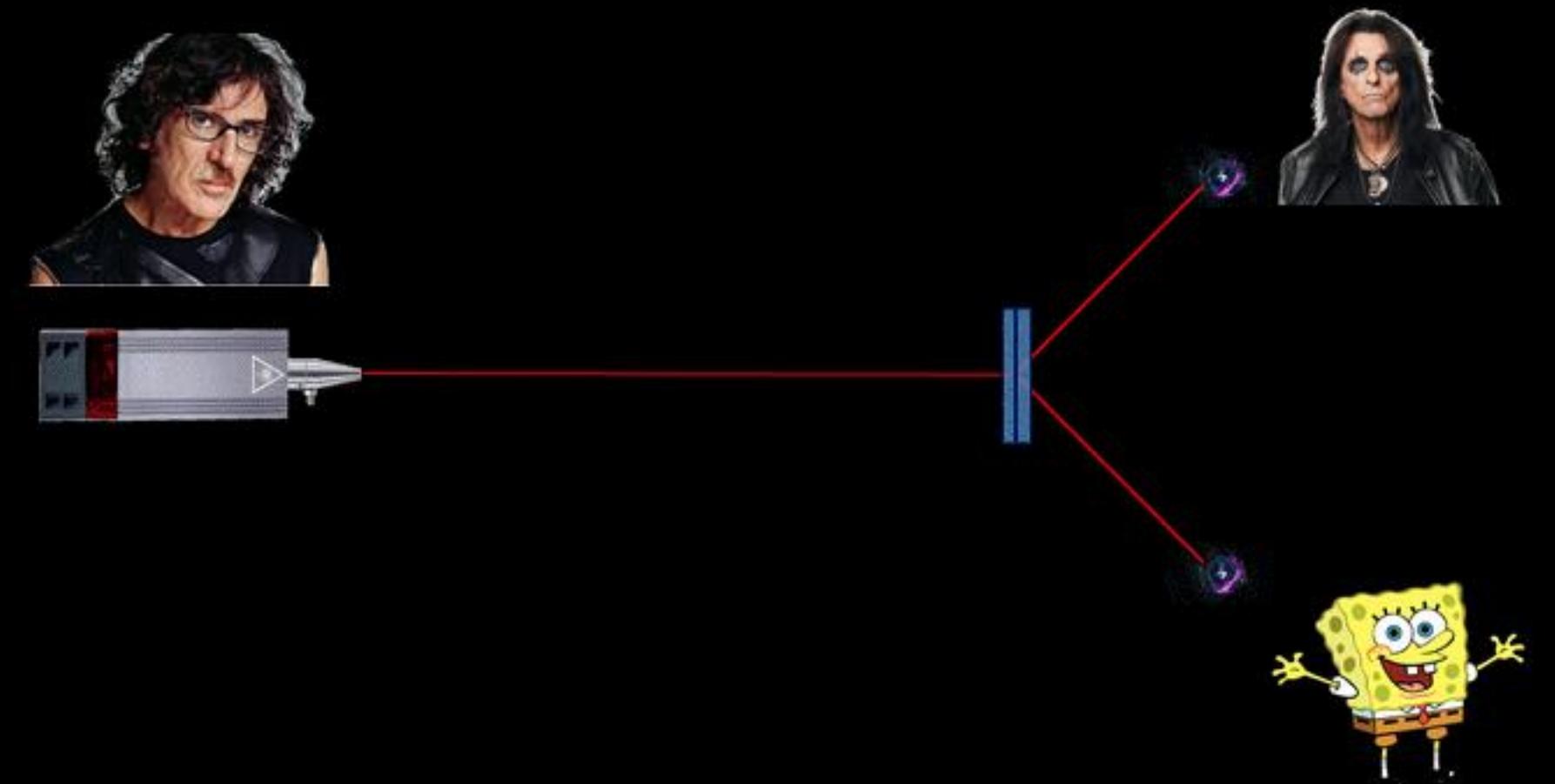


## ► COMUNICACION CUANTICA



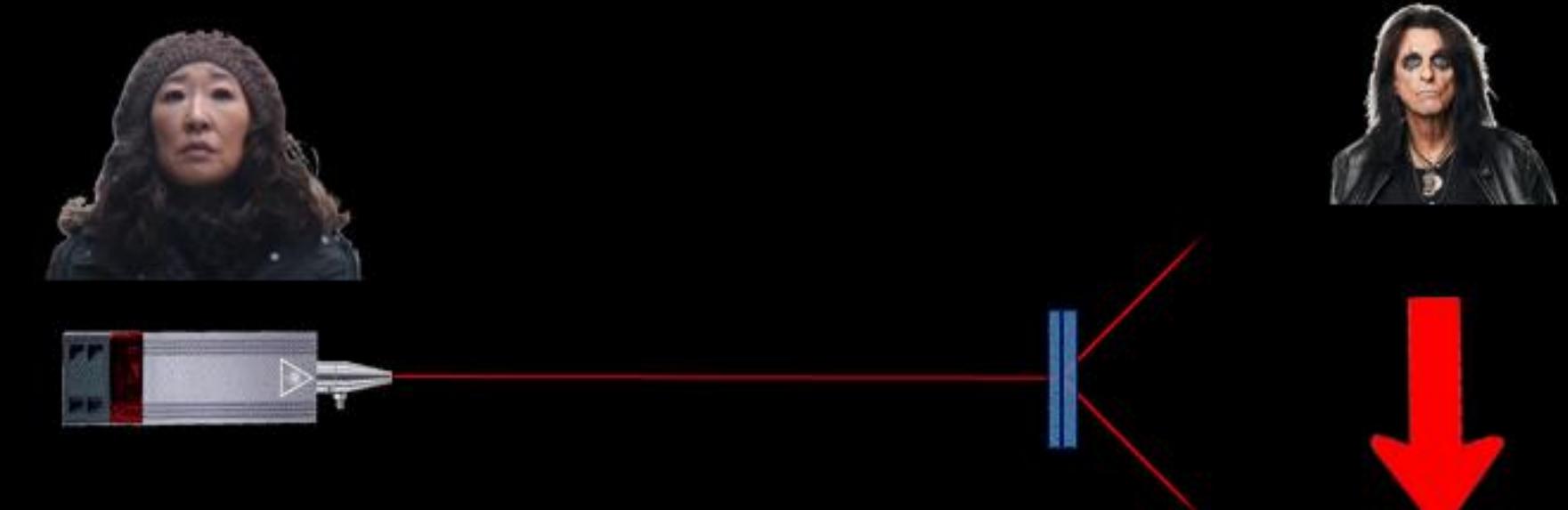
►SUPER -DENSE CODING

Transmitir 2 bits clásicos con 1 qubit.



»**SUPER -DENSE CODING**

Transmitir 2 bits clásicos con 1 qubit.



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

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

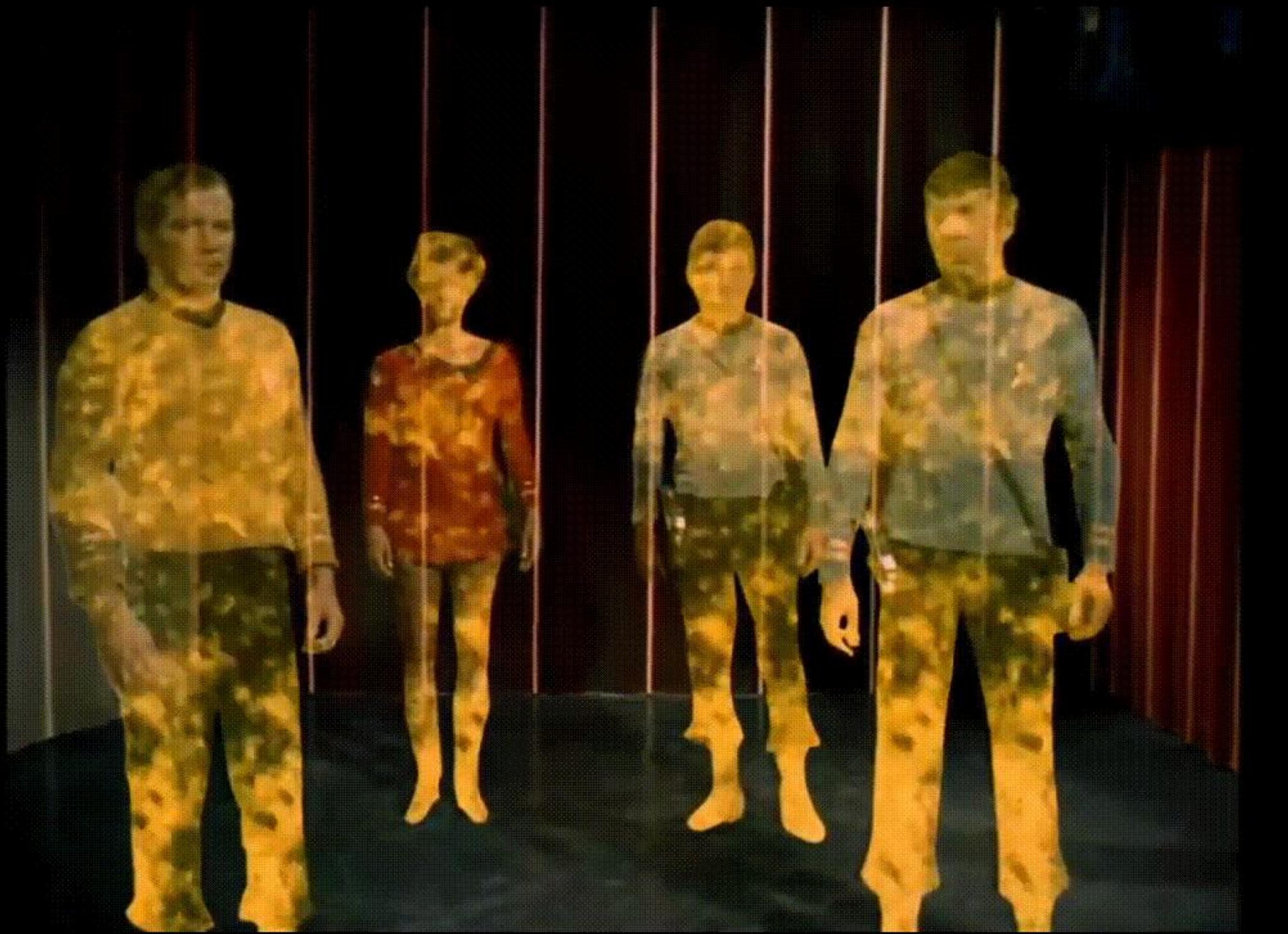
$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

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

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	$ZX$	$- 10\rangle +  01\rangle$

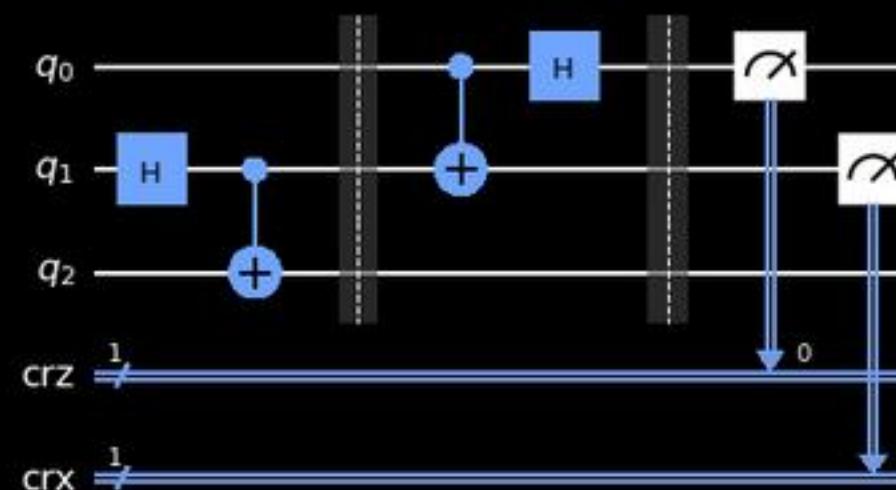
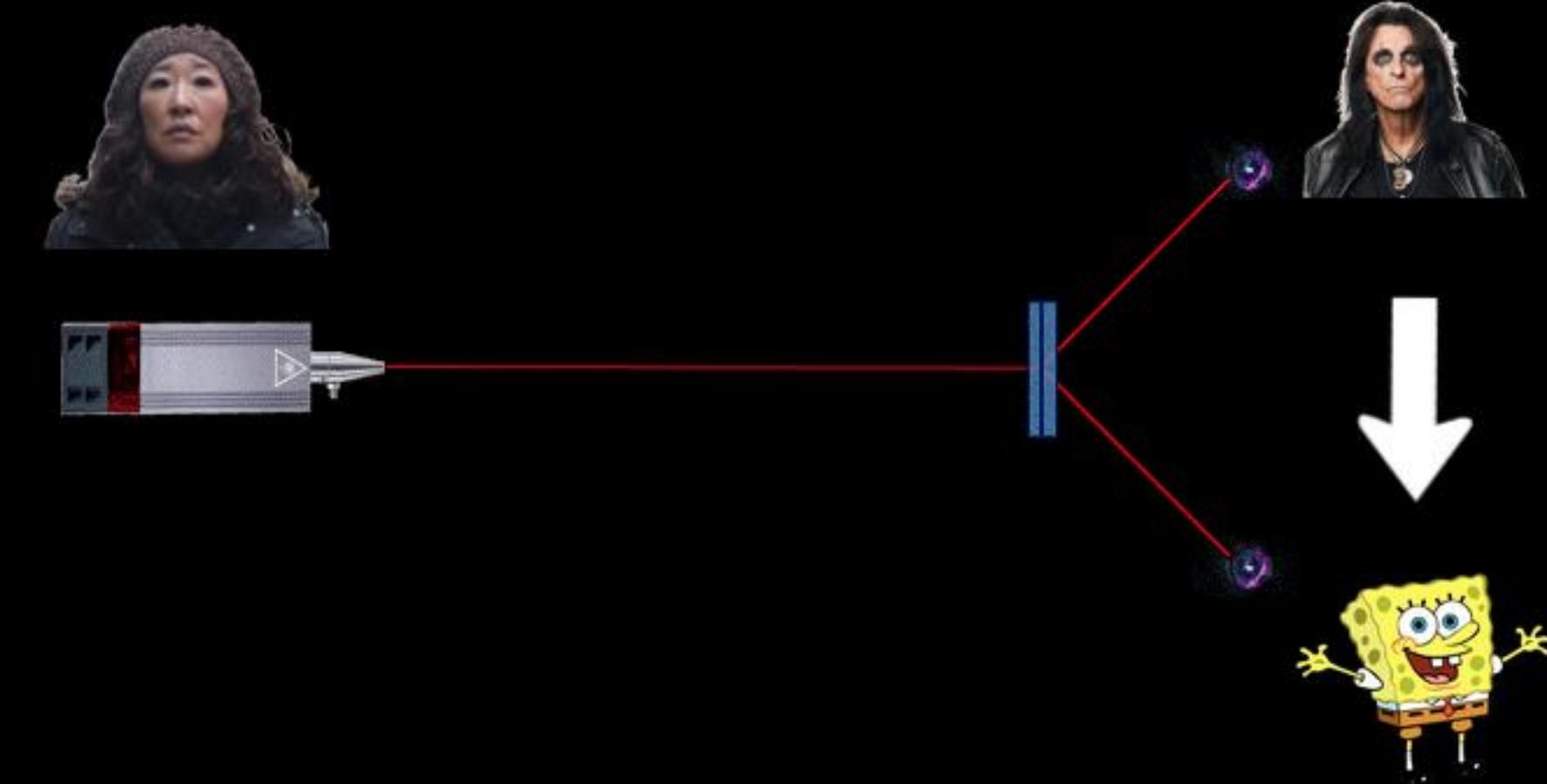
Bob Receives ( $\cdot \frac{1}{\sqrt{2}}$ )	After CNOT-gate ( $\cdot \frac{1}{\sqrt{2}}$ )	After H-gate
$ 00\rangle +  11\rangle$	$ 00\rangle +  10\rangle$	$ 00\rangle$
$ 10\rangle +  01\rangle$	$ 11\rangle +  01\rangle$	$ 01\rangle$
$ 00\rangle -  11\rangle$	$ 00\rangle -  10\rangle$	$ 10\rangle$
$-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

► SUPER - DENSE CODING



➡ TELEPORTATION

Transmitir 1 qubit, usando 2 bits clásicos.



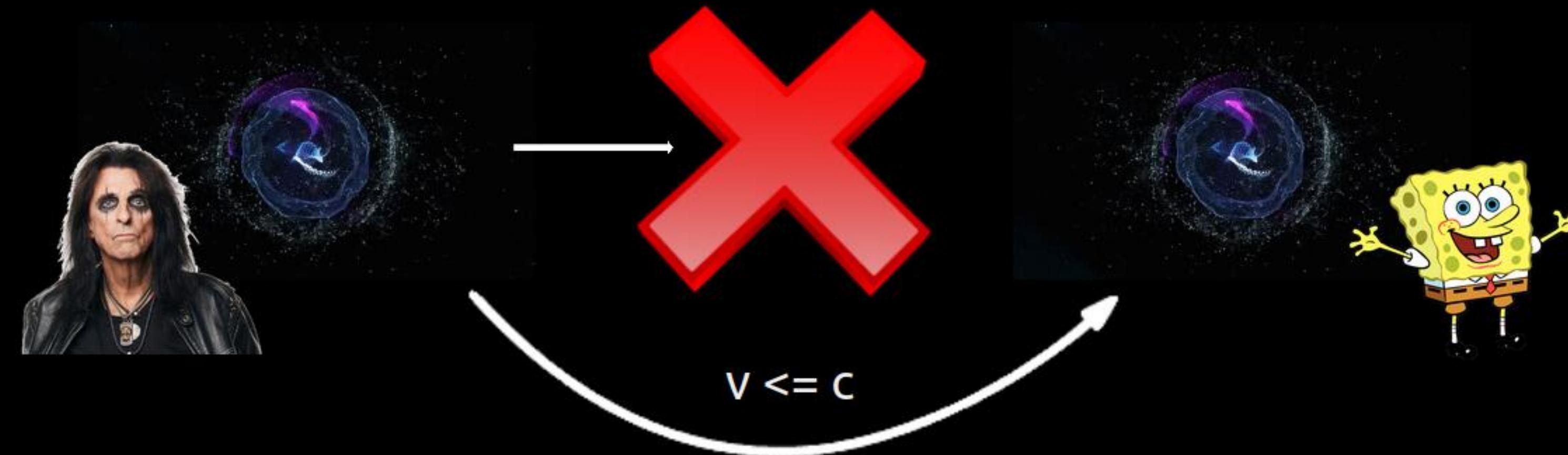
00 → Do nothing

01 → Apply  $X$  gate

10 → Apply  $Z$  gate

11 → Apply  $ZX$  gate

➡ TELEPORTATION



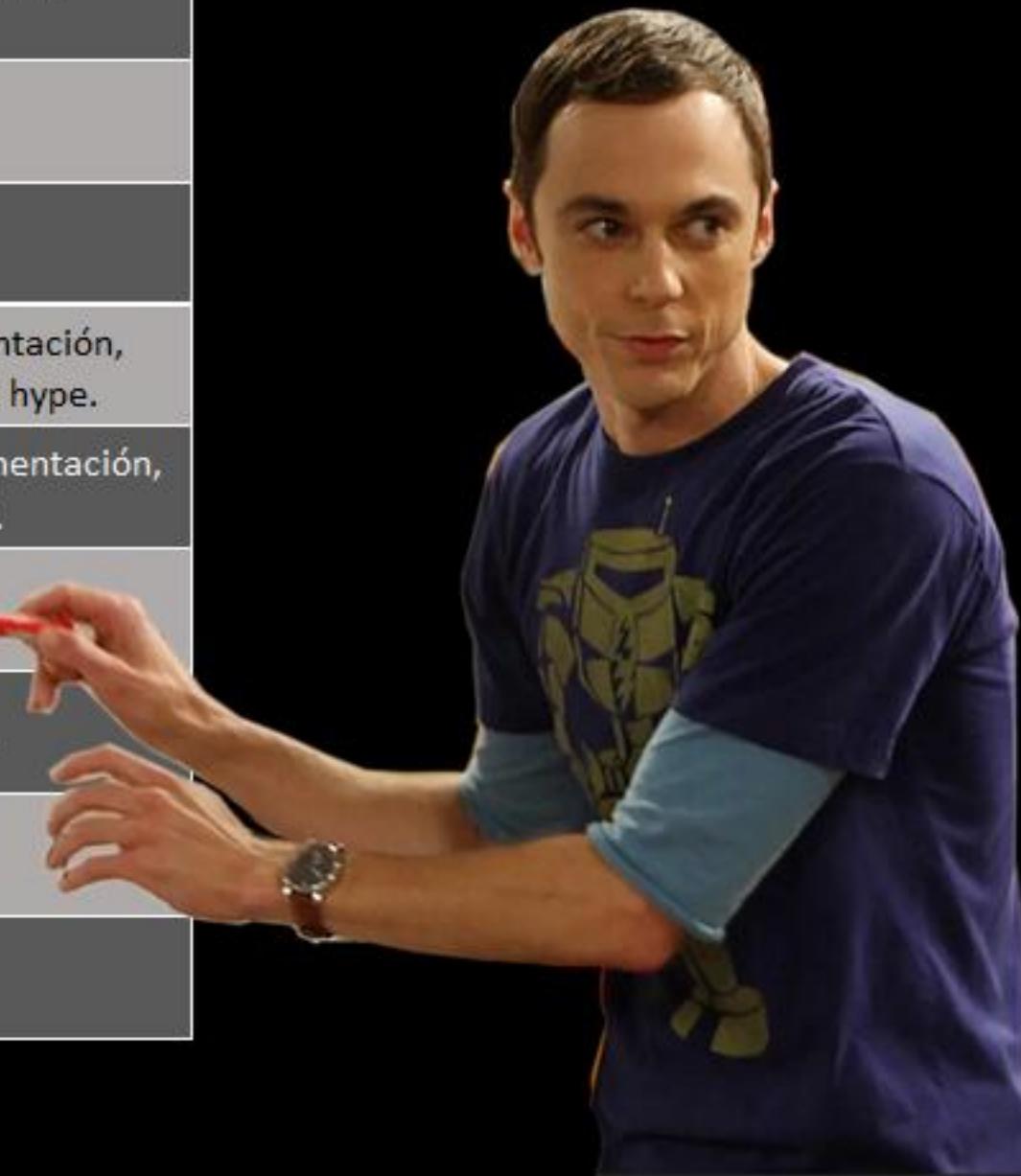
Hey Bob! please check...

➡ 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.
	Superdense Coding	Transmisión segura, codificar 2 bits en 1 qubit.	+++	--	Todavía teórico.
Comunicación cuántica	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](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/prabSTRACT/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>