TAURUS

# The Quantum Computing Risk & Post-Quantum Cryptography


JP Aumasson

https://aumasson.jp

AMERICAN UNIVERSITY OF BEIRUT


# Background

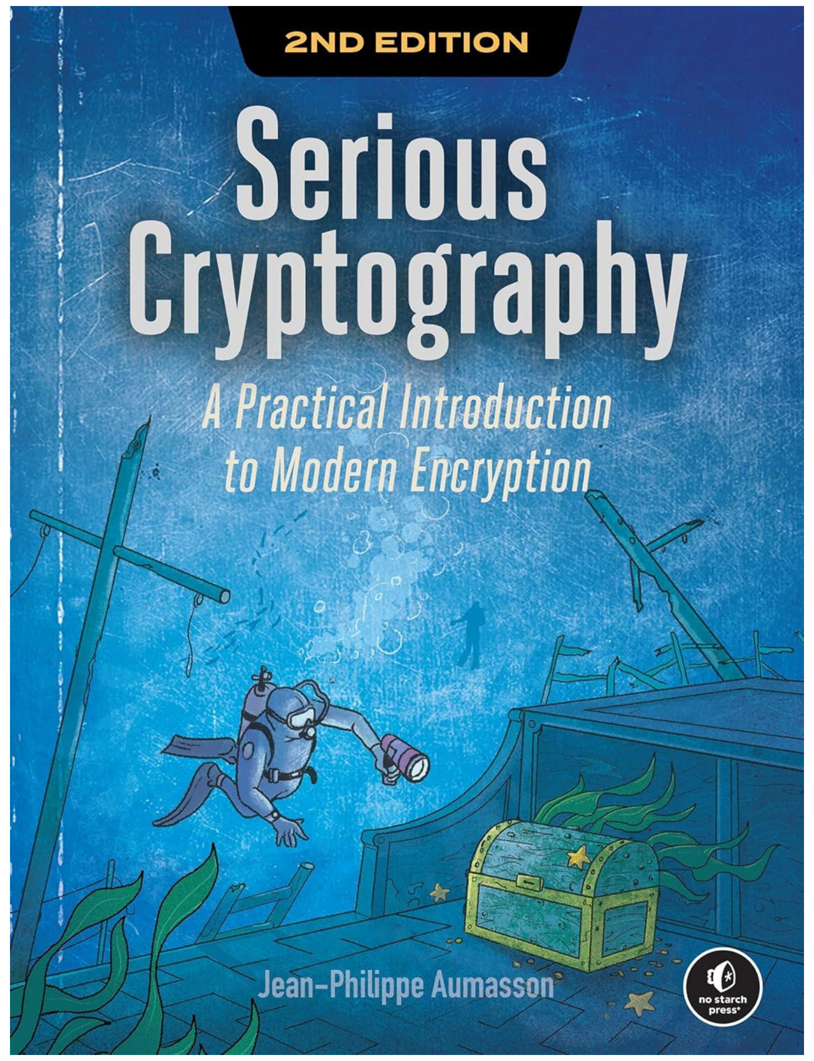
Co-founder & chief security officer of **Taurus SA**

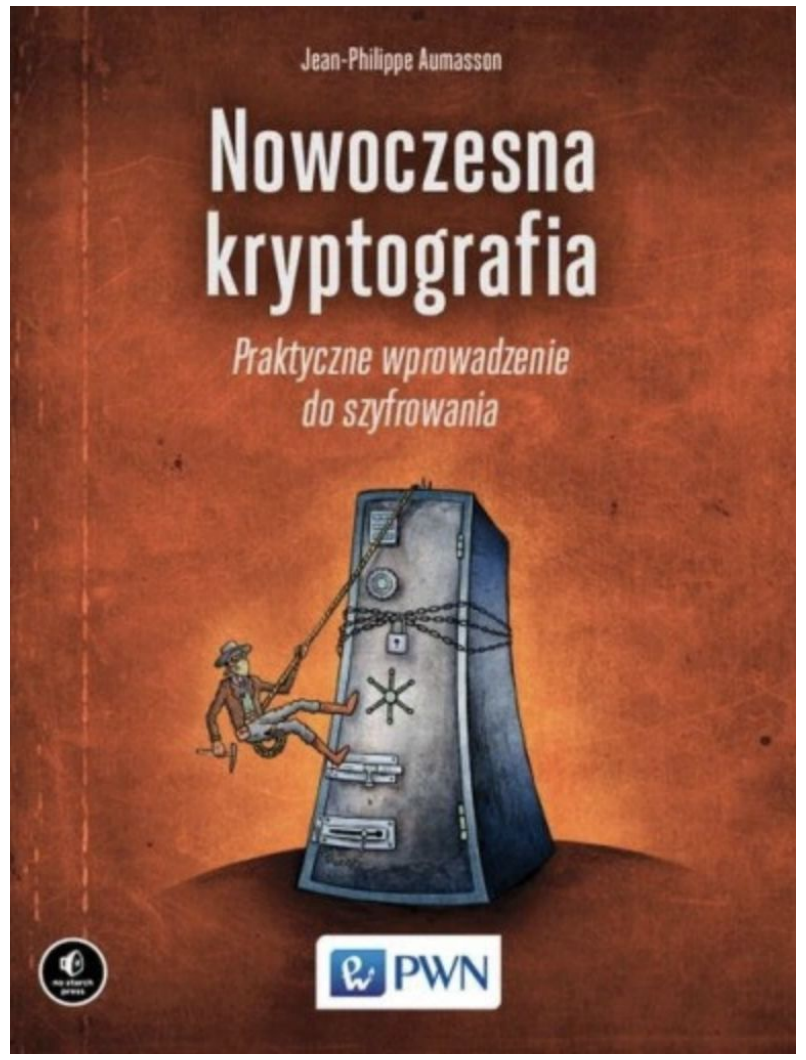
- Fintech founded in 2018, team of 90+
- **Digital asset custody** infrastructure
- Cool tech: HSMs, HA infra, smart contracts, etc.

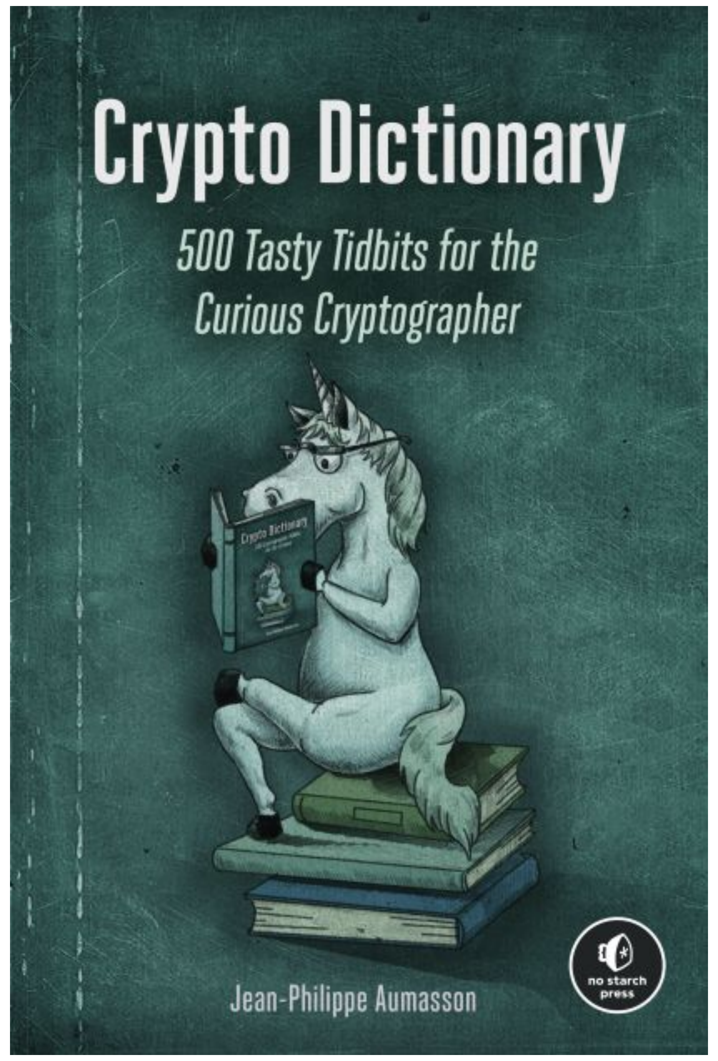
https://taurushq.com https://t-dx.com


- 20 years in cryptography & security
- Designed industry standards
- Crypto*graphy* books

https://aumasson.jp



# Quantum physics

**Explains how Nature behaves at the smallest scales** (atoms, electrons, photons)

It defies common sense:

- Particles can behave like waves (**wave-particle duality**)
- A particle is in an uncertain state until it's observed (**superposition**)
- Particles at large distances appear to influence one another (**non-locality**)

**Simulating** quantum physics involves complex equations of complexity growing exponentially, **practically impossible** even with supercomputers

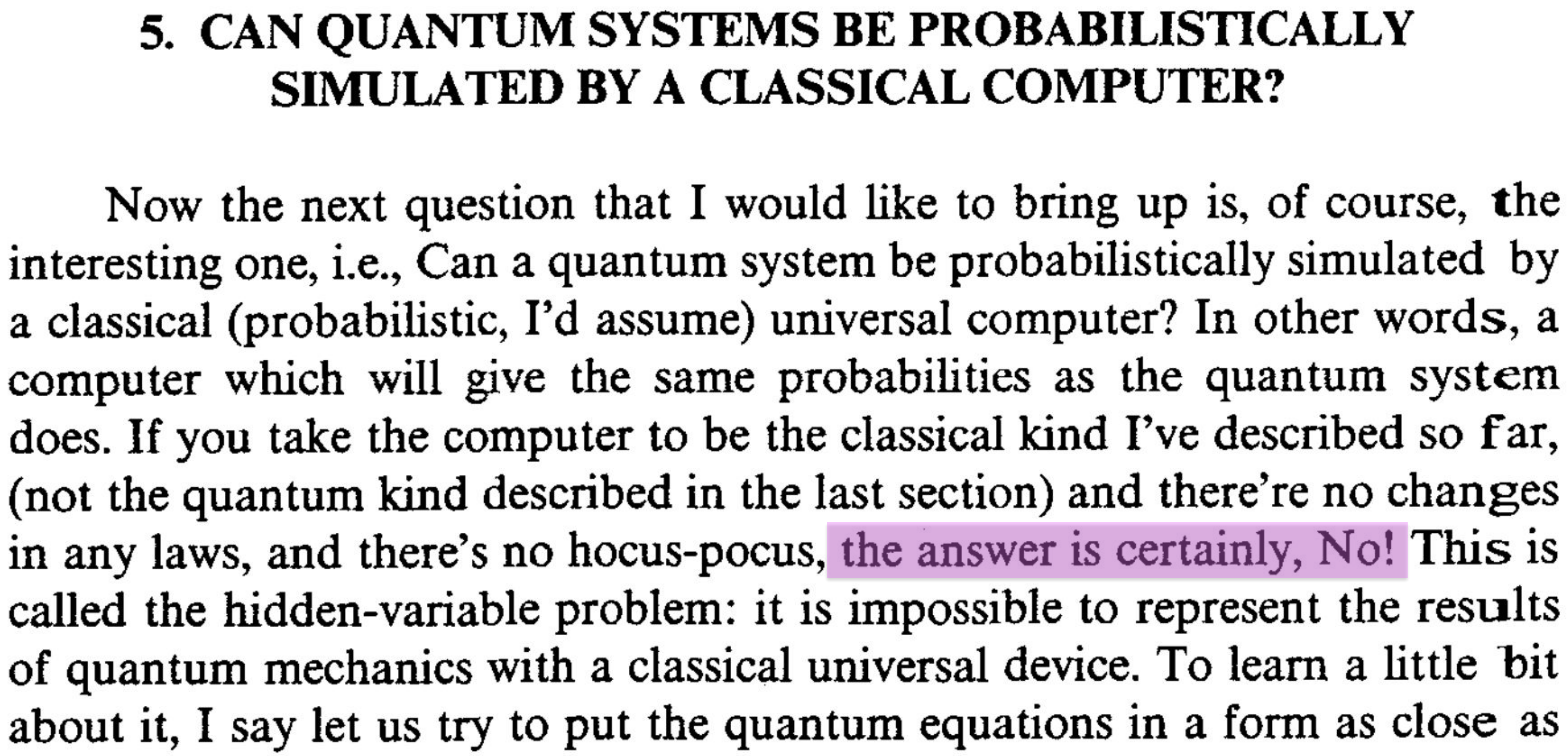
# Simulating Physics with Computers

**Richard P. Feynman**

*Department of Physics, California Institute of Technology, Pasadena, California 91107*

*Received May 7, 1981*

# Not to break crypto..



## 5. CAN QUANTUM SYSTEMS BE PROBABILISTICALLY SIMULATED BY A CLASSICAL COMPUTER?

Now the next question that I would like to bring up is, of course, the interesting one, i.e., Can a quantum system be probabilistically simulated by a classical (probabilistic, I'd assume) universal computer? In other words, a computer which will give the same probabilities as the quantum system does. If you take the computer to be the classical kind I've described so far, (not the quantum kind described in the last section) and there're no changes in any laws, and there's no hocus-pocus, the answer is certainly, No! This is called the hidden-variable problem: it is impossible to represent the results of quantum mechanics with a classical universal device. To learn a little bit about it, I say let us try to put the quantum equations in a form as close as

# … but simulate quantum physics

## 4. QUANTUM COMPUTERS—UNIVERSAL QUANTUM SIMULATORS

The first branch, one you might call a side-remark, is, Can you do it with a new kind of computer—a quantum computer? (I'll come back to the other branch in a moment.) Now it turns out, as far as I can tell, that you can simulate this with a quantum system, with quantum computer elements. It's not a Turing machine, but a machine of a different kind. If we disregard the continuity of space and make it discrete, and so on, as an approximation (the same way as we allowed ourselves in the classical case), it does seem to

# Quantum bits (qubits)

**Superposition** state $\alpha \, |0\rangle + \beta \, |1\rangle$

*Observation, random outcome*

0 with probability $|\alpha|^2$

1 with probability $|\beta|^2$


*α, β are "probabilities" called **amplitudes***
*(can be complex, and negative numbers)*

Once observed, a qubit stays 0 or 1 forever

# Different math, different computing

## ON THE POWER OF QUANTUM COMPUTATION

DANIEL R. SIMON
MICROSOFT CORP.
ONE MICROSOFT WAY
REDMOND WA 98052-6399

DANSIMON@MICROSOFT.COM

**Abstract.** The quantum model of computation is a model, analogous to the probabilistic Turing Machine, in which the normal laws of chance are replaced by those obeyed by particles on a quantum mechanical scale, rather than the rules familiar to us from the macroscopic world. We present here a problem of distinguishing between two fairly natural classes of function, which can provably be solved exponentially faster in the quantum model than in the classical probabilistic one, when the function is given as an oracle drawn equiprobably from the uniform distribution on either class. We thus offer compelling evidence that the quantum model may have significantly more complexity theoretic power than the probabilistic Turing Machine. In fact, drawing on this work, Shor has recently developed remarkable new quantum polynomial-time algorithms for the discrete logarithm and integer factoring problems.

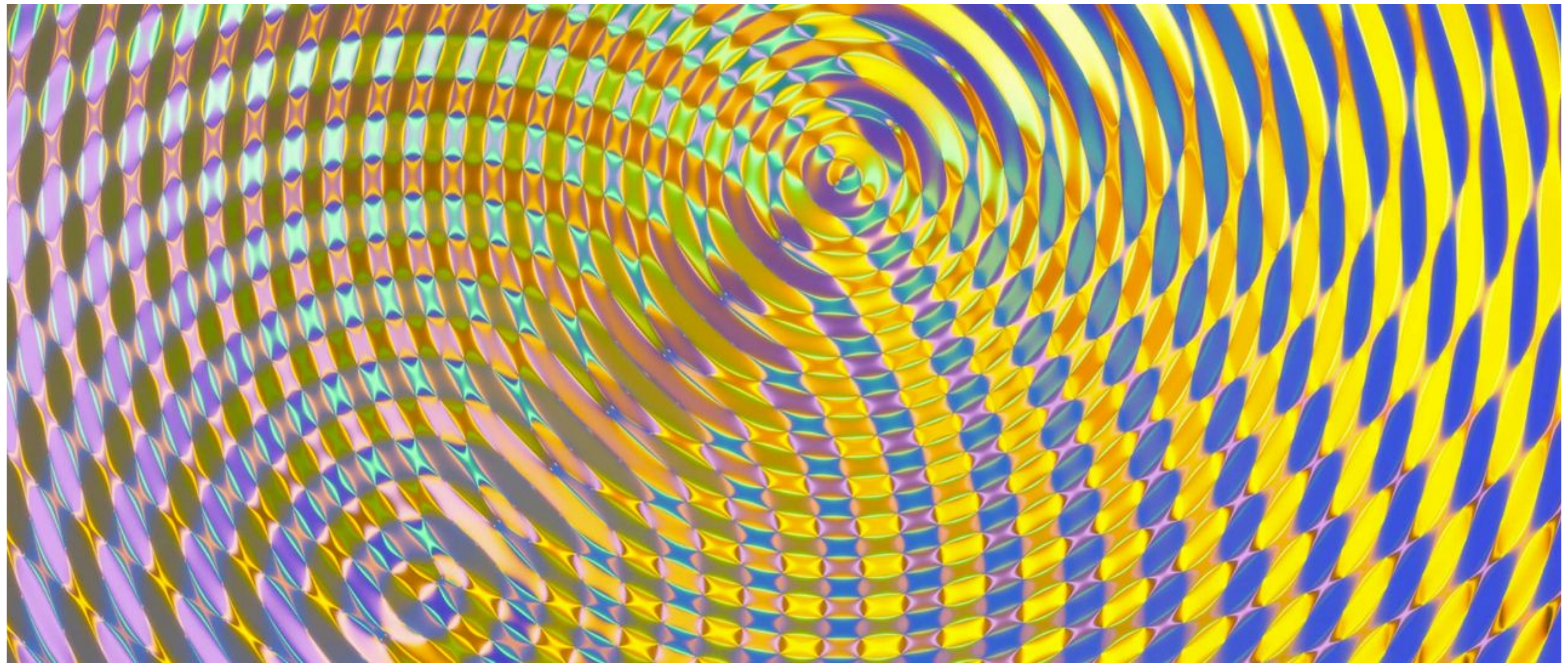
**1. Introduction.** *You have nothing to do but mention the quantum theory, and people will take your voice for the voice of science, and believe anything.*

—Bernard Shaw, *Geneva* (1938)

# Quantum computing’s power

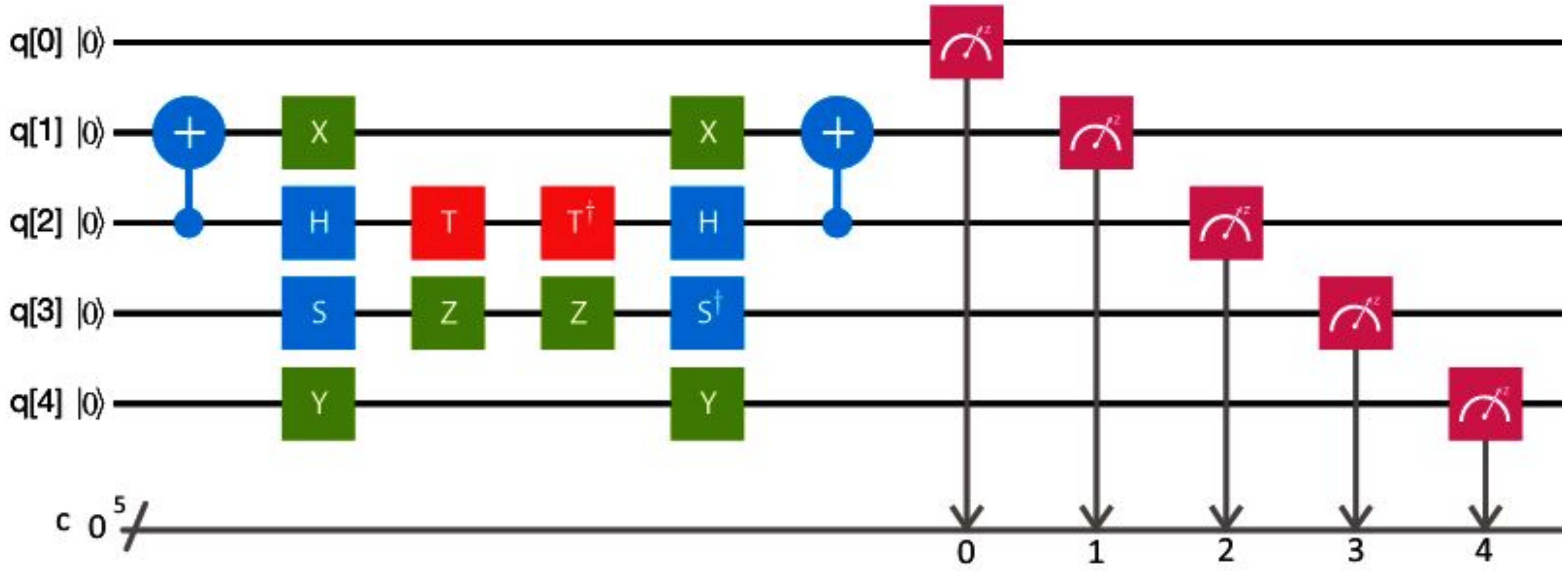
Quantum computing draws its power mainly from two phenomena:

- **Entanglement**, whereby distant particles are "correlated" and *appear* to influence each other even at large distances. (Cf. EPR paradox.)
- **Interference**, which lets quantum algorithms amplify correct answers and cancel out wrong ones, by arranging how their probability amplitudes combine.



# Quantum algorithms

**Circuits** of quantum gates, transforming a quantum state, ending with an observation



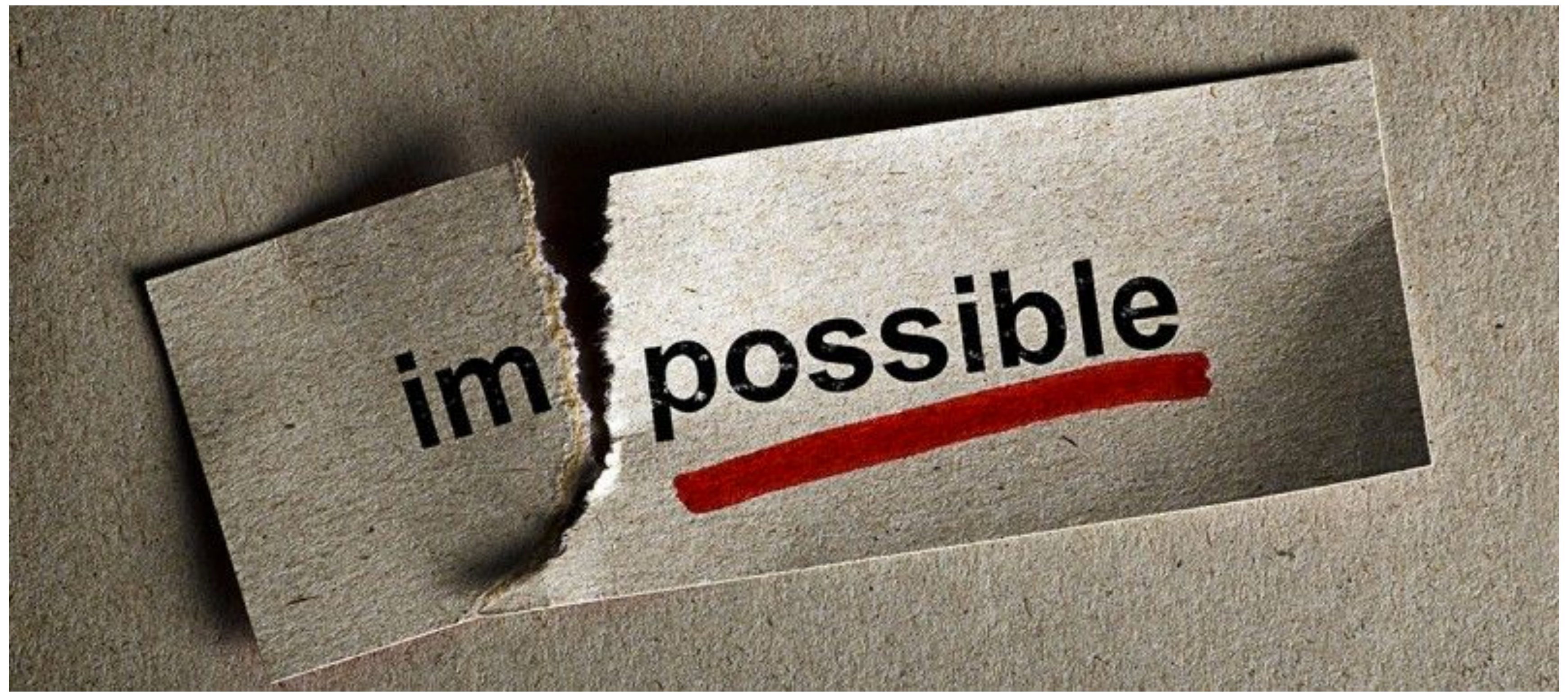

Can be simulated with basic linear algebra  but does no scale, exponential cost:

- **Quantum state** = vector of $2^N$ amplitudes for N qubits
- **Quantum gates** = matrix multiplications, with $O(2^{3N})$ complexity

# Quantum speedup

When quantum computers can solve a problem faster than classical computers

Most interesting: **Superpolynomial** quantum speedup (“exponential" boost)




List of problems on the **Quantum Zoo**: http://math.nist.gov/quantum/zoo/

# Quantum parallelism

Quantum computers “work" on all values simultaneously, via **superposition**

But they do not *“try every answer in parallel and pick the best”*

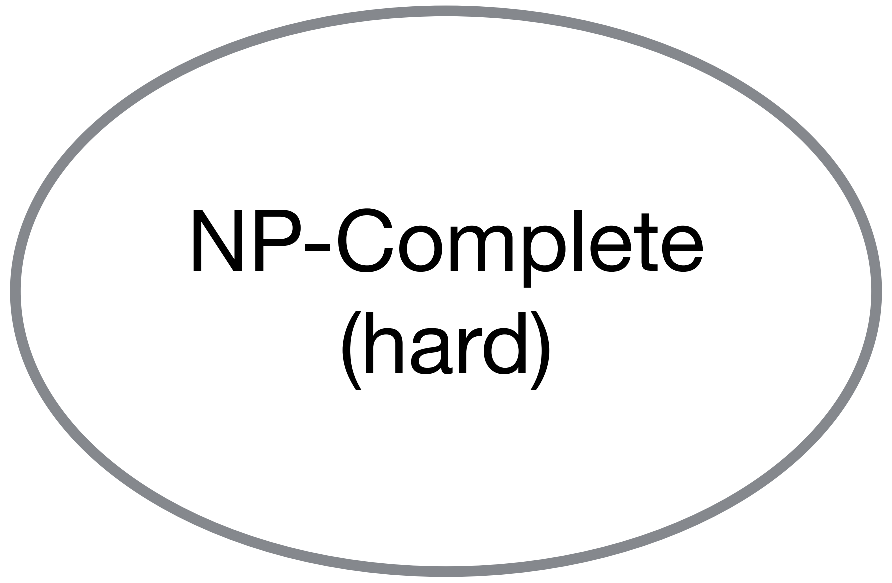
You can only **observe one “value”** that results from the interference of all, as a projection from the Hilbert space where qubits “live" to some basis

# Most hard problems don’t benefit from QC

NP-hard problems are very common:

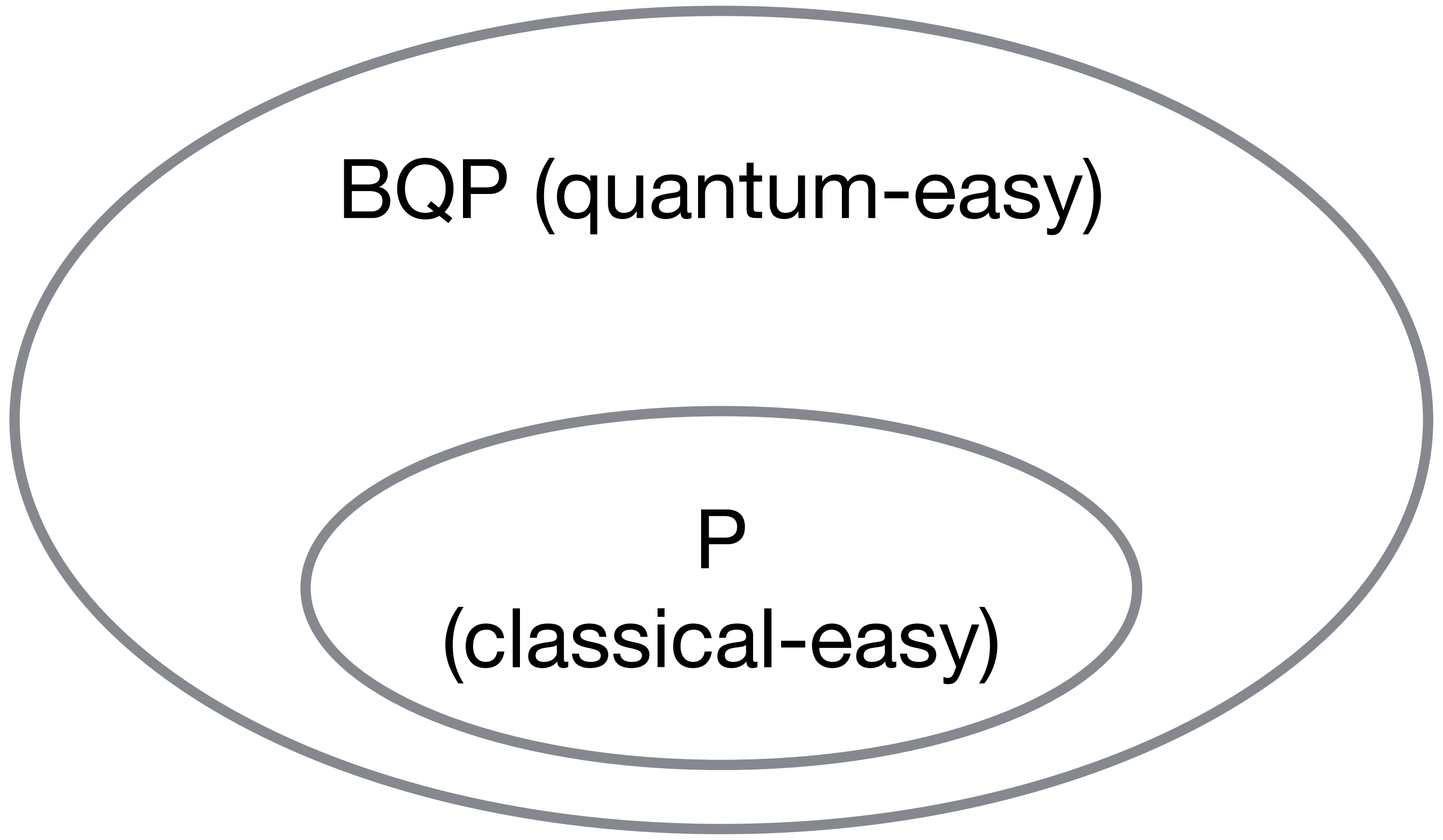
- Problems whose solution is **hard to find, but easy to verify**
- Structured like constraint satisfaction problems (scheduling, puzzle-solving, etc.)

**CANNOT be solved faster** with quantum computers!



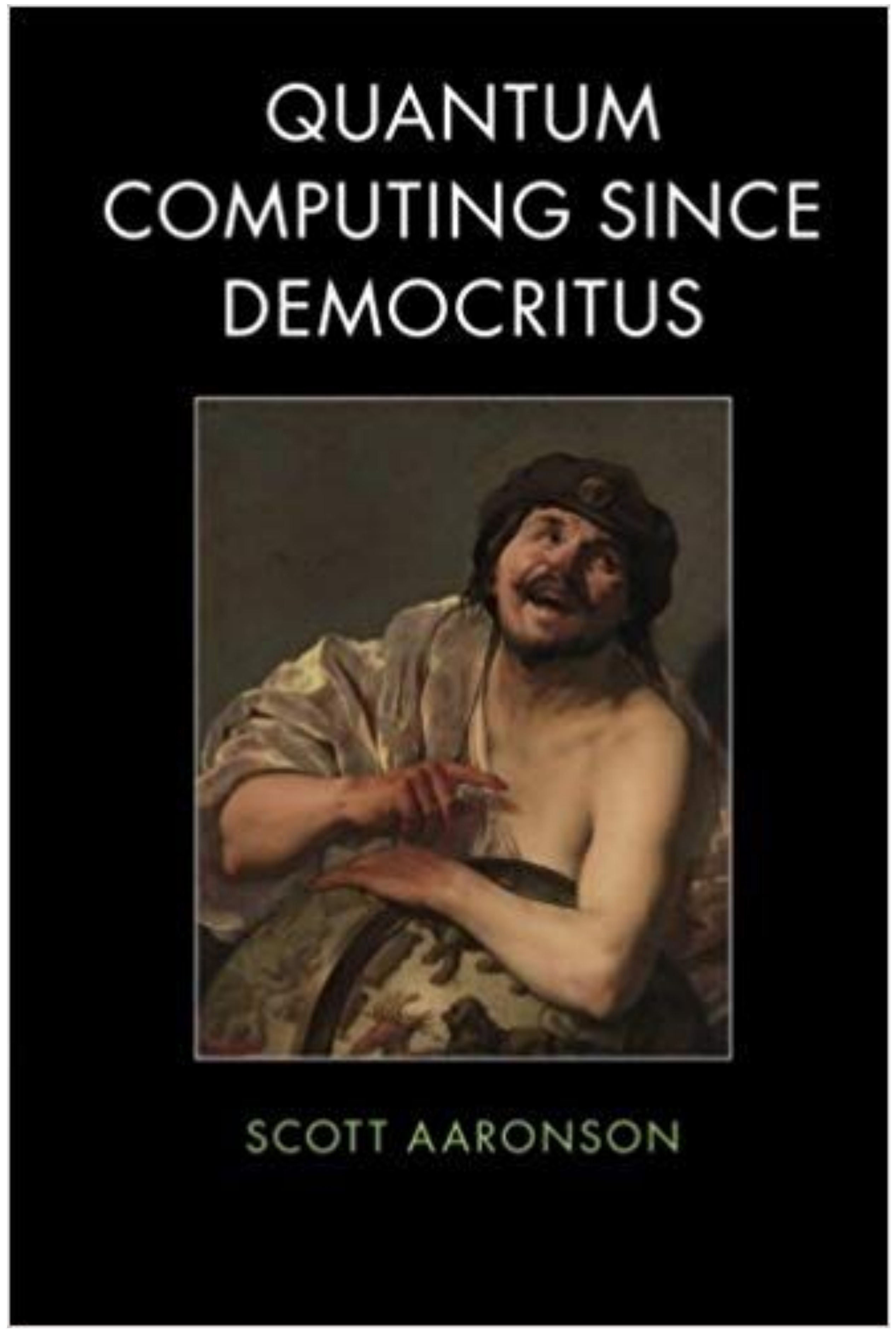

**NP is not in BQP (most likely!)**

Therefore quantum computers can’t solve NP-hard problems



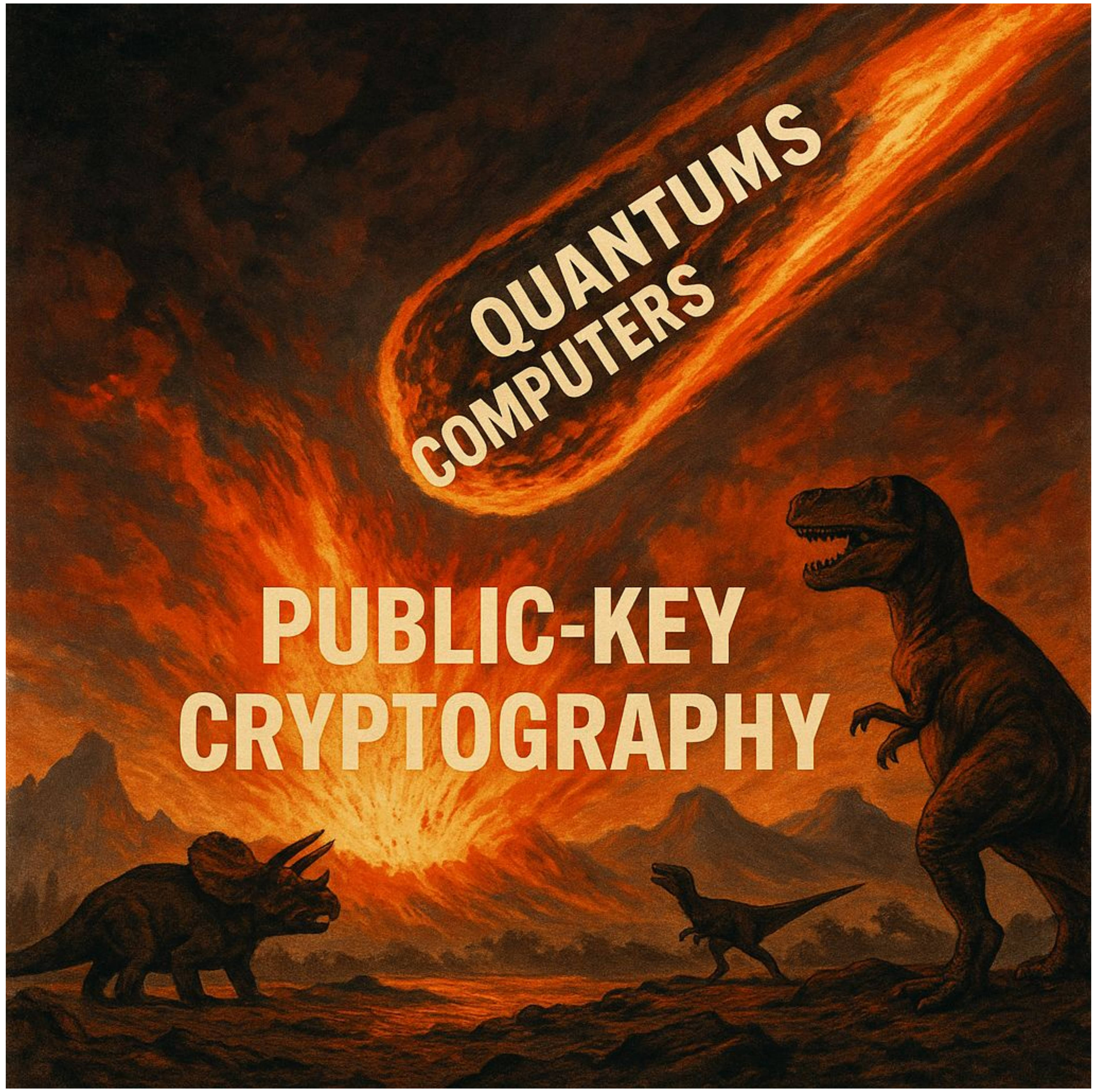

**BQP** = bounded-error quantum polynomial time, what QC can solve efficiently

# Recommended reading




**Contents**

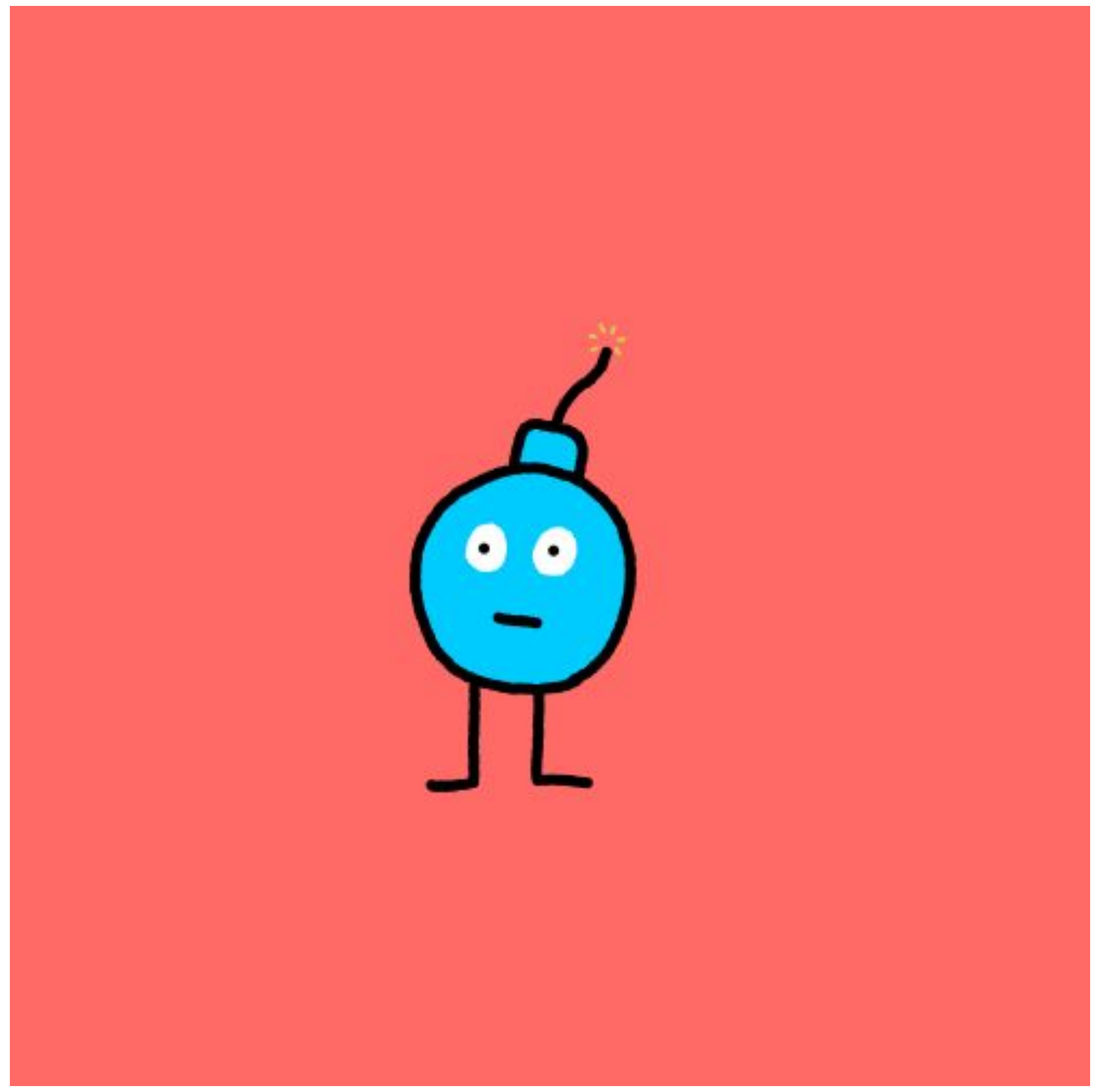
# Impact on cryptography



# Shor's quantum algorithm

Polynomial-time algorithm for the following problems:

- Computes **p** given **n** = **pq** → RSA dead
- Computes **d** given **y** = $\mathbf{x}^{\mathbf{d}}$ mod **p** → ECC/DH dead

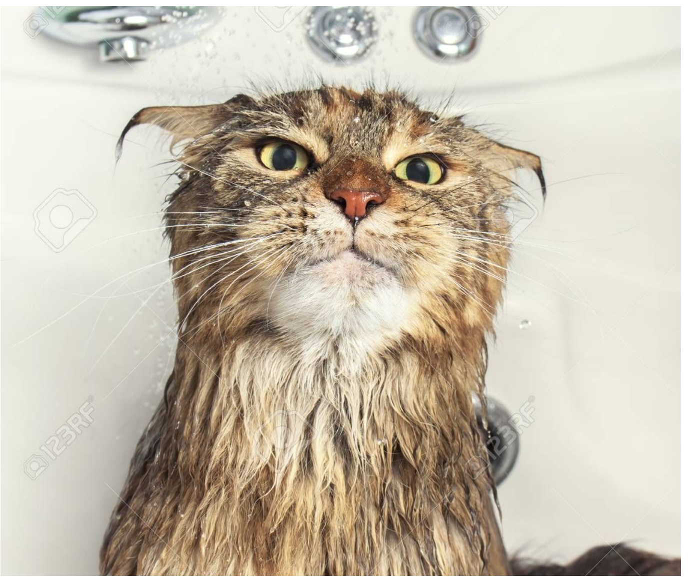


***Practically impossible*** on a classical machine

#QuantumSpeedup

# How bad for crypto?

Worse



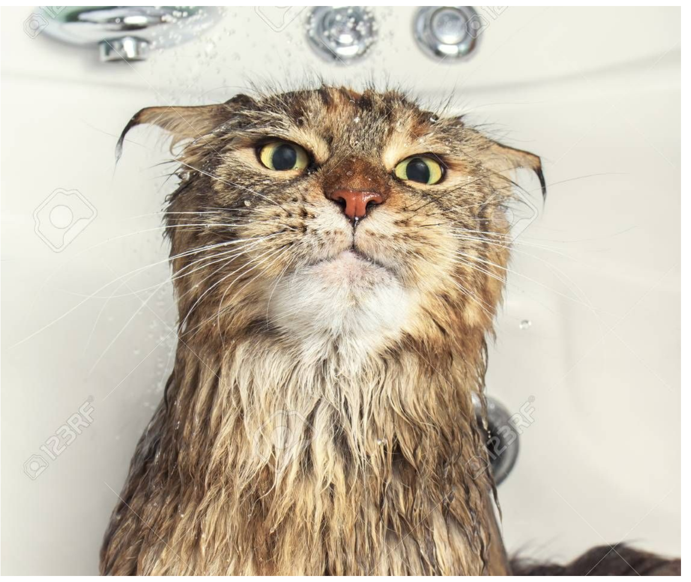
**Mild: <u>Signatures</u>** (ECDSA, Ed25519, etc.)
Broken sigs can be reissued with a post-quantum algorithm

**Bad: <u>Key agreement</u>** (Diffie-Hellman, ECDH, etc.)
Partially mitigated by secret internal states and reseeding

**Terrible: <u>Encryption</u>** (RSA encryption, ECIES, etc.)
Encrypted messages compromised forever

# Concretely

Worse



**Mild: <u>Signatures</u>**
PKI certificates, code signing, blockchain transactions, etc.
*Migration planned, technology ready*

**Bad: <u>Key agreement</u>**
TLS, IPsec, WireGuard, e2ee messaging (WhatsApp, Signal), etc.
*Migration ongoing (e.g. Apple’s iMessage, Cloudflare, etc.)*

**Terrible: <u>Encryption</u>**
Key encapsulation, some encrypted backups, PGP messages, etc.
*Migration to prioritize*

# Not there yet

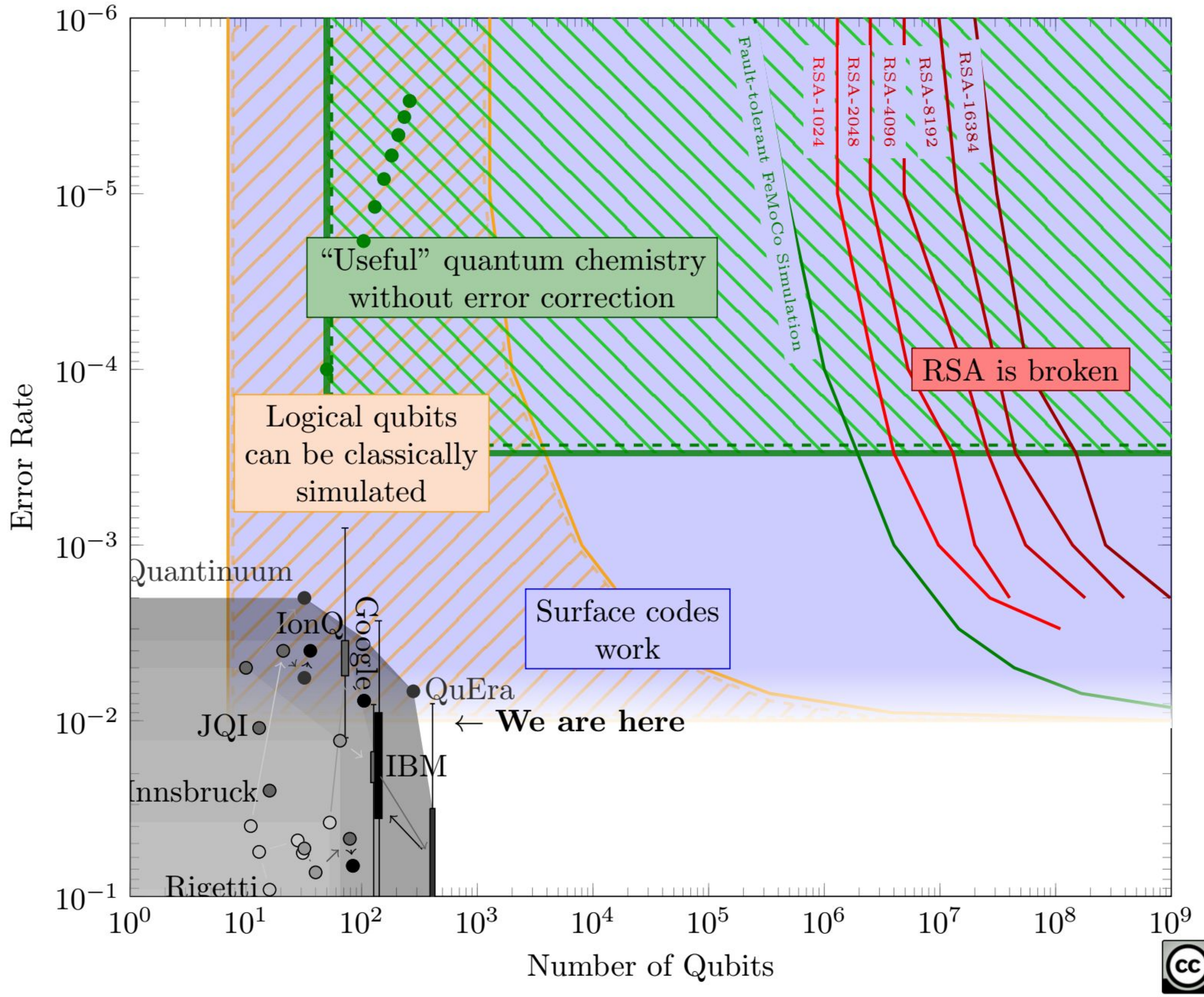
**Millions** of qubits to break RSA, to implement **error correction**

QC in its infancy, only research prototypes useless in practice

**Google and IBM** leading

2 main dimensions:

- Error rate
- Qubits number (physical, logical)






https://sam-jaques.appspot.com/quantum_landscape_2024

# Beware PR content

Often hyperbolic, misleading claims from QC companies

JD Supra

Quantum Leap: Google Claims Its New Quantum Computer Provides Evidence That We Live in a Multiverse

Google's latest refinement to its quantum computer, Willow, may represent such a moment. By achieving computational feats once thought to be confined to...

8 Jan 2025

PCMag

Google's Quantum Chip Can Do in 5 Minutes What Would Take Other Computers 10 Septillion Years

Google's quantum computing division unveiled a new chip, dubbed Willow, that the tech giant says makes it infinitely faster and better than existing...

10 Dec 2024

## Google's Quantum Chip Can Do in 5 Minutes What Would Take Other Computers 10 Septillion Years

Google makes a quantum leap that suggests we may live in a multiverse.

By Kate Irwin Dec 10, 2024

## Harnessing a new type of material

All of today's announcements build on our team's recent breakthrough: the world's first topoconductor. This revolutionary class of materials enables us to create *topological superconductivity*, a new state of matter that previously existed only in theory. The advance stems from Microsoft's innovations in the design and fabrication of gate-defined devices that combine indium arsenide (a semiconductor) and aluminum (a superconductor). When cooled to near absolute zero and tuned with magnetic fields,

# IBM's roadmap

https://www.ibm.com/roadmaps/quantum/

## 2026

**Demonstrate first example of scientific quantum advantage and a fault-tolerant module.**

We will demonstrate the first examples of quantum advantage using a quantum computer with HPC.

## 2027

**Diversify quantum advantage and entangle fault-tolerant modules.**

The scale, quality, speed of the quantum computer will improve to allow executing quantum circuits at a scale of 10K gates on a 1000+ qubits.

## 2029

**Deliver the first fault-tolerant quantum computer.**

The first fault-tolerant quantum computer will be available to clients and allow execution of 100M gates on 200 qubits.

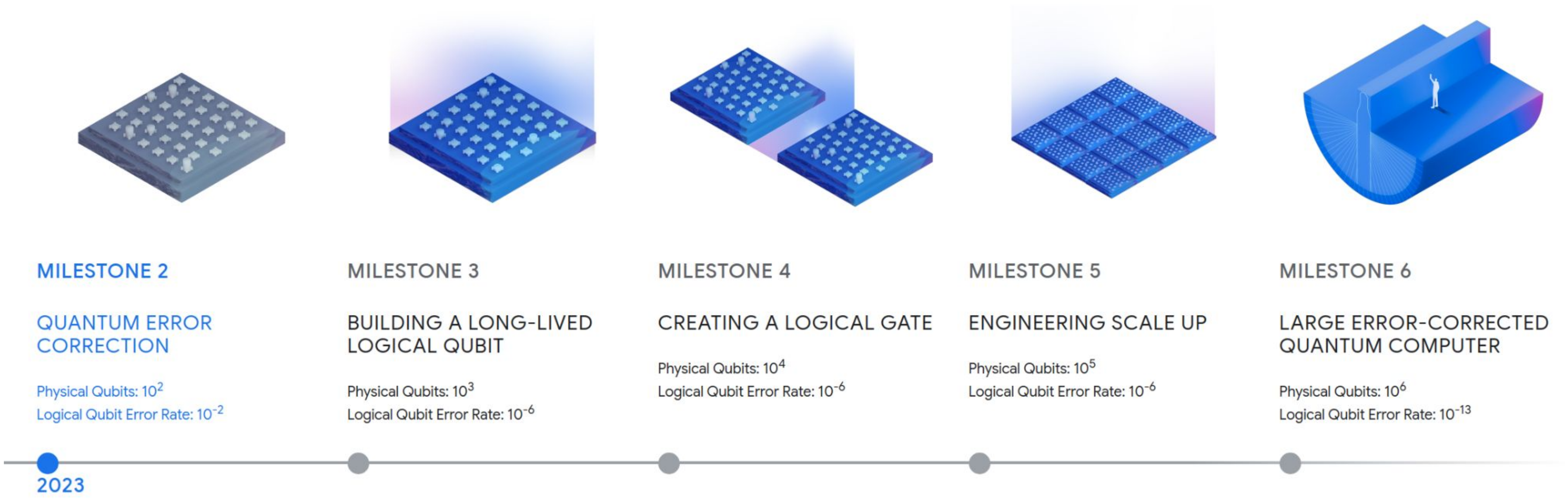
## 2033+

**Unlock the full power of quantum computing at scale.**

Scale fault-tolerant quantum computers to run circuits of 1 billion gates on up to 2000 qubits, unlocking the full power of quantum computing.

# Google's roadmap

https://quantumai.google/roadmap



# Quantum supremacy?

## Google thinks it's close to "quantum supremacy." Here's what that really means.

It's not the number of qubits; it's what you do with them that counts.

by Martin Giles and Will Knight March 9, 2018

**Seventy-two may not be a large number, but in quantum** computing terms, it's massive. This week Google unveiled Bristlecone, a new quantum computing chip with 72 quantum bits, or qubits—the fundamental units of computation

# When it Looks too Good to be True..

**Factoring 2 048 RSA integers in 177 days with 13 436 qubits and a multimode memory**

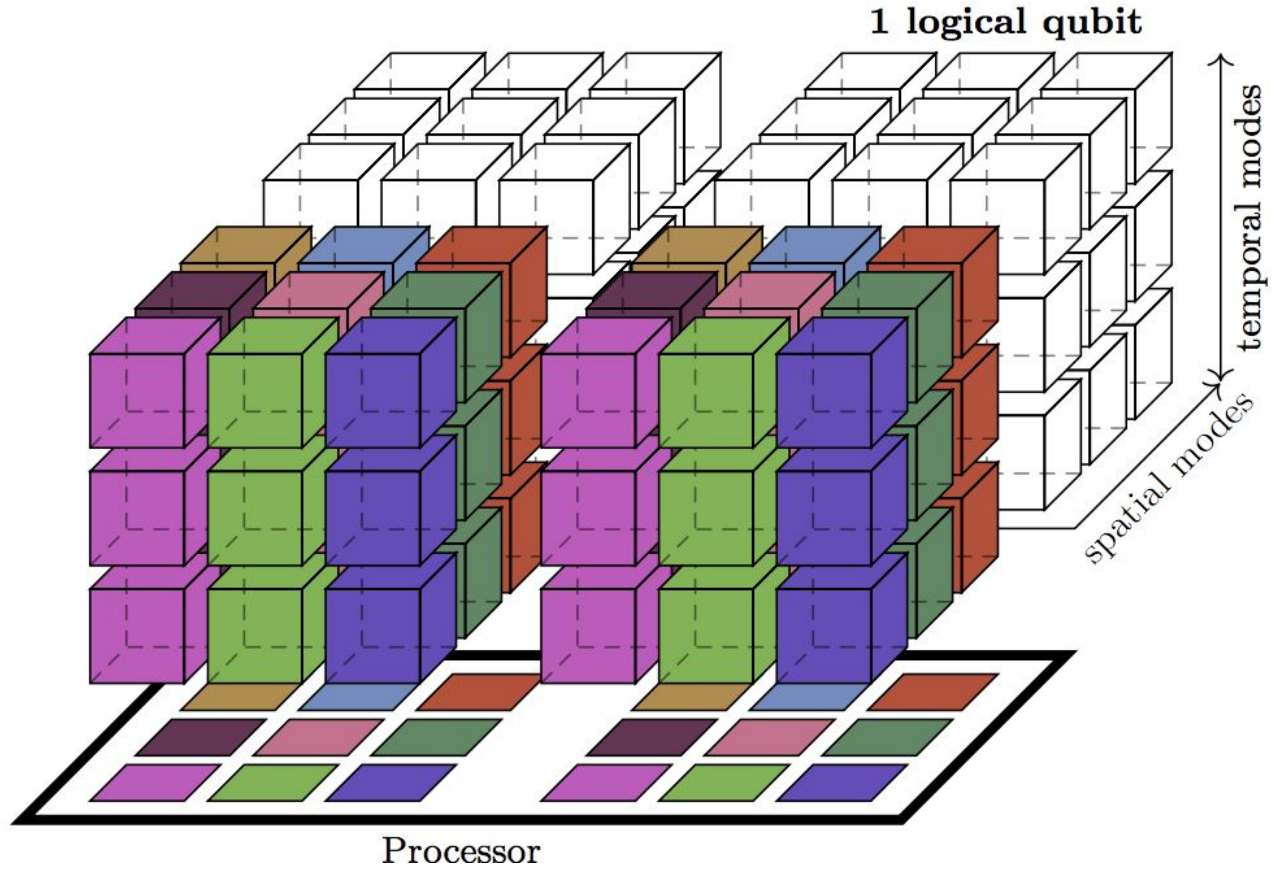
Élie Gouzien* and Nicolas Sangouard†
*Université Paris–Saclay, CEA, CNRS, Institut de physique théorique, 91 191 Gif-sur-Yvette, France*
(Dated: March 11, 2021)

We analyze the performance of a quantum computer architecture combining a small processor and a storage unit. By focusing on integer factorization, we show a reduction by several orders of magnitude of the number of processing qubits compared to a standard architecture using a planar grid of qubits with nearest-neighbor connectivity. This is achieved by taking benefit of a temporally and spatially multiplexed memory to store the qubit states between processing steps. Concretely, for a characteristic physical gate error rate of $10^{-3}$, a processor cycle time of 1 microsecond, factoring a 2 048 bits RSA integer is shown possible in 177 days with a processor made with 13 436 physical qubits and a multimode memory with 2 hours storage time. By inserting additional error-correction steps, storage times of 1 second are shown to be sufficient at the cost of increasing the runtime by about 23 %. Shorter runtimes (and storage times) are achievable by increasing the number of qubits in the processing unit. We suggest realizing such an architecture using a microwave interface between a processor made with superconducting qubits and a multiplexed memory using the principle of photon echo in solids doped with rare-earth ions.



*Introduction* — Superconducting qubits form the building blocks of one of the most advanced platforms for realizing quantum computers [1]. The standard architecture consists in laying superconducting qubits in a 2D grid and making the computation using only neighboring interactions. Recent estimations showed however that fault-tolerant realizations of various quantum algorithms with this architecture would require millions physical qubits [2–4]. These performance analyses naturally raise the question of an architecture better exploiting the potential of superconducting qubits.

In developing a quantum computer architecture we




Sam Jaques
@sejaques

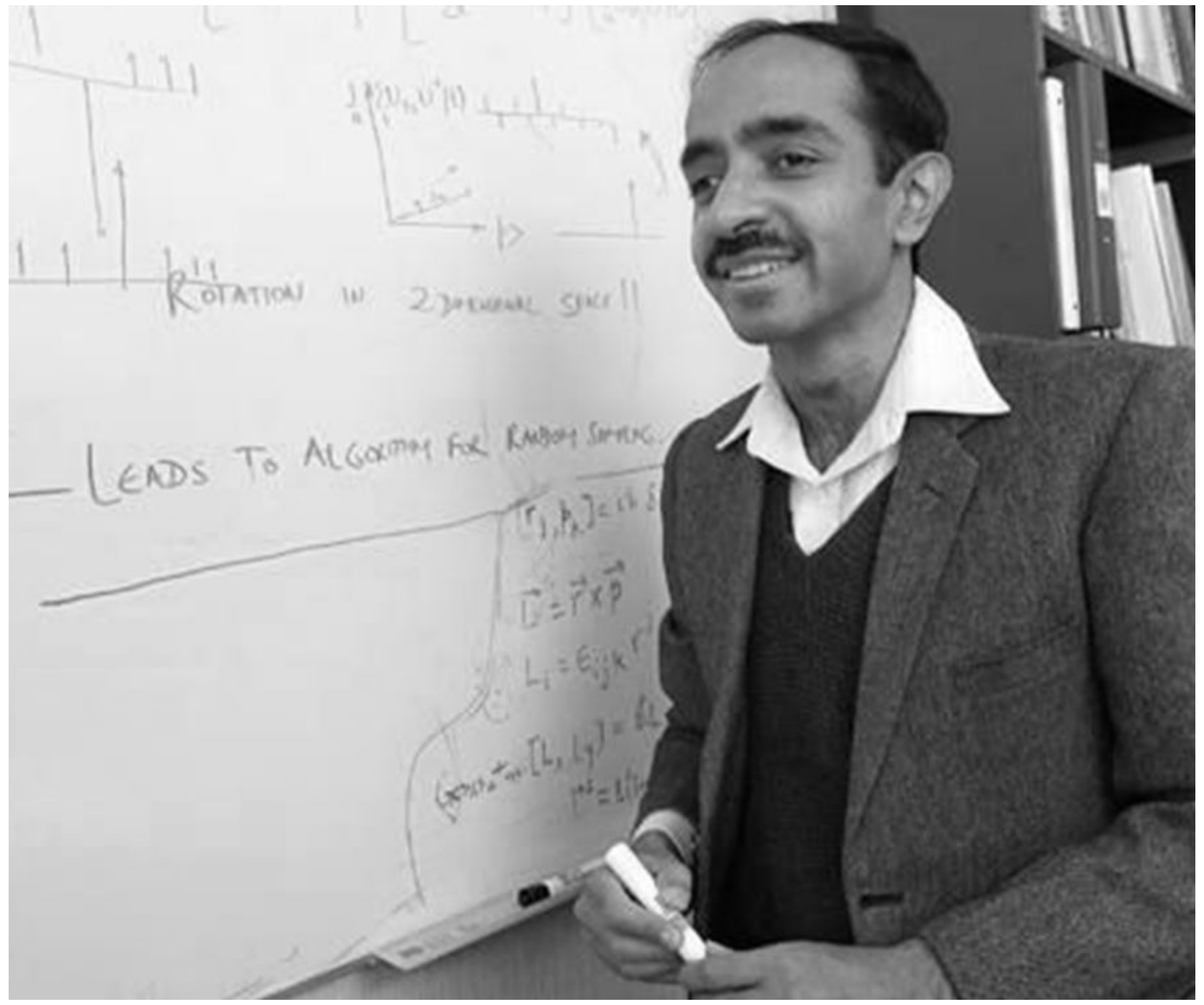
Replying to @veorq

Very important caveat: it needs 430 million "memory qubits"

Craig Gidney @CraigGidney · Mar 15
Replying to @quantumVerd @KikeSolanoPhys and 4 others
The paper uses a cost model where quantum memory is comparatively cheap. I'd have included the mem qubit count in the title (at n=2048 there's 13K compute qubits and 430M mem qubits) but don't see anything wrong with considering a world where mem ends up cheaper than cpu.

# Quantum search

Impacts symmetric cryptography



Grover's algorithm (1996)

Searches in N items in $\sqrt{N}$ queries!

- AES-128 broken in $\sqrt{(2^{128})} = 2^{64}$ operations?
- Applications in machine learning models

**Caveats**:

- Constant factor in **O(√N)** may be huge
- Doesn't parallelize as classical search does

# Quantum-searching AES keys

| | #gates | | depth | | #qubits |
|---|---|---|---|---|---|
| $k$ | $T$ | Clifford | $T$ | overall | |
| 128 | $1.19 \cdot 2^{86}$ | $1.55 \cdot 2^{86}$ | $1.06 \cdot 2^{80}$ | $1.16 \cdot 2^{81}$ | 2, 953 |
| 192 | $1.81 \cdot 2^{118}$ | $1.17 \cdot 2^{119}$ | $1.21 \cdot 2^{112}$ | $1.33 \cdot 2^{113}$ | 4, 449 |
| 256 | $1.41 \cdot 2^{151}$ | $1.83 \cdot 2^{151}$ | $1.44 \cdot 2^{144}$ | $1.57 \cdot 2^{145}$ | 6,681 |

**Table 5.** Quantum resource estimates for Grover's algorithm to attack AES-$k$, where $k \in \{128, 192, 256\}$.

https://arxiv.org/pdf/1512.04965v1.pdf

If gates are the size of a hydrogen atom (12pm) this depth is the **diameter of the solar system** (~$10^{13}$m), yet less than 5 grams

More efficient circuits will be designed…

# Quantum-searching AES keys

From February 2020, better circuits found

**Implementing Grover oracles for quantum key search on AES and LowMC**

Samuel Jaques[1*†], Michael Naehrig[2], Martin Roetteler[3], and Fernando Virdia[4†‡]

| scheme | $r$ | #Clifford | $\#T$ | $\#M$ | $T$-depth | full depth | width | $G$-cost | $DW$-cost | $p_s$ |
|---|---|---|---|---|---|---|---|---|---|---|
| AES-128 | 1 | $1.13 \cdot 2^{82}$ | $1.32 \cdot 2^{79}$ | $1.32 \cdot 2^{77}$ | $1.48 \cdot 2^{70}$ | $1.08 \cdot 2^{75}$ | 1665 | $1.33 \cdot 2^{82}$ | $1.76 \cdot 2^{85}$ | $1/e$ |
| AES-128 | 2 | $1.13 \cdot 2^{83}$ | $1.32 \cdot 2^{80}$ | $1.32 \cdot 2^{78}$ | $1.48 \cdot 2^{70}$ | $1.08 \cdot 2^{75}$ | 3329 | $1.34 \cdot 2^{83}$ | $1.75 \cdot 2^{86}$ | 1 |
| AES-192 | 2 | $1.27 \cdot 2^{115}$ | $1.47 \cdot 2^{112}$ | $1.47 \cdot 2^{110}$ | $1.47 \cdot 2^{102}$ | $1.14 \cdot 2^{107}$ | 3969 | $1.50 \cdot 2^{115}$ | $1.11 \cdot 2^{119}$ | 1 |
| AES-256 | 2 | $1.56 \cdot 2^{147}$ | $1.81 \cdot 2^{144}$ | $1.81 \cdot 2^{142}$ | $1.55 \cdot 2^{134}$ | $1.29 \cdot 2^{139}$ | 4609 | $1.84 \cdot 2^{147}$ | $1.45 \cdot 2^{151}$ | $1/e$ |
| AES-256 | 3 | $1.17 \cdot 2^{148}$ | $1.36 \cdot 2^{145}$ | $1.36 \cdot 2^{143}$ | $1.55 \cdot 2^{134}$ | $1.28 \cdot 2^{139}$ | 6913 | $1.38 \cdot 2^{148}$ | $1.08 \cdot 2^{152}$ | 1 |

# Eliminating the Problem: 256-bit Keys

# Defeating Quantum Algorithms


A.k.a. “quantum-safe”, “quantum-resilient”

Must not rely on factoring or discrete logarithm

# Why bother?

**Insurance** against QC threat:

- "QC has a probability *p* work in year X and the impact would be $N for us"
- "I'd like to eliminate this risk and I'm ready to spend $M for it"

Supposedly the motivation of USG/NSA:

"*we anticipate a need to shift to quantum-resistant cryptography in the near future.*" — NSA in CNSS advisory 02-2015

# NSA's Take (Aug 2021)

**Q: Is NSA worried about the threat posed by a potential quantum computer because a CRQC exists?**
A: NSA does not know when or even if a quantum computer of sufficient size and power to exploit public key cryptography (a CRQC) will exist.

**Q: Why does NSA care about quantum computing today? Isn't quantum computing a long way off?**
A: The cryptographic systems that NSA produces, certifies, and supports often have very long lifecycles. NSA has to produce requirements today for systems that will be used for many decades in the future, and data protected by these systems will still require cryptographic protection for decades after these solutions are replaced. There is growing research in the area of quantum computing, and global interest in its pursuit have provoked NSA to ensure the enduring protection of NSS by encouraging the development of post-quantum cryptographic standards and planning for an eventual transition.

**Q: What are the timeframes in NSS for deployment of new algorithms, use of equipment, and national security information intelligence value?**
A: New cryptography can take 20 years or more to be fully deployed to all National Security Systems. NSS equipment is often used for decades after deployment. National security information intelligence value varies depending on classification, sensitivity, and subject, but it can require protection for many decades.

https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.pdf

# The NIST competition

CSRC HOME > GROUPS > CT > POST-QUANTUM CRYPTOGRAPHY PROJECT

## POST-QUANTUM CRYPTO PROJECT

***NEWS -- August 2, 2016:*** The National Institute of Standards and Technology (NIST) is requesting comments on a new process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. Please see the Post-Quantum Cryptography Standardization menu at left.

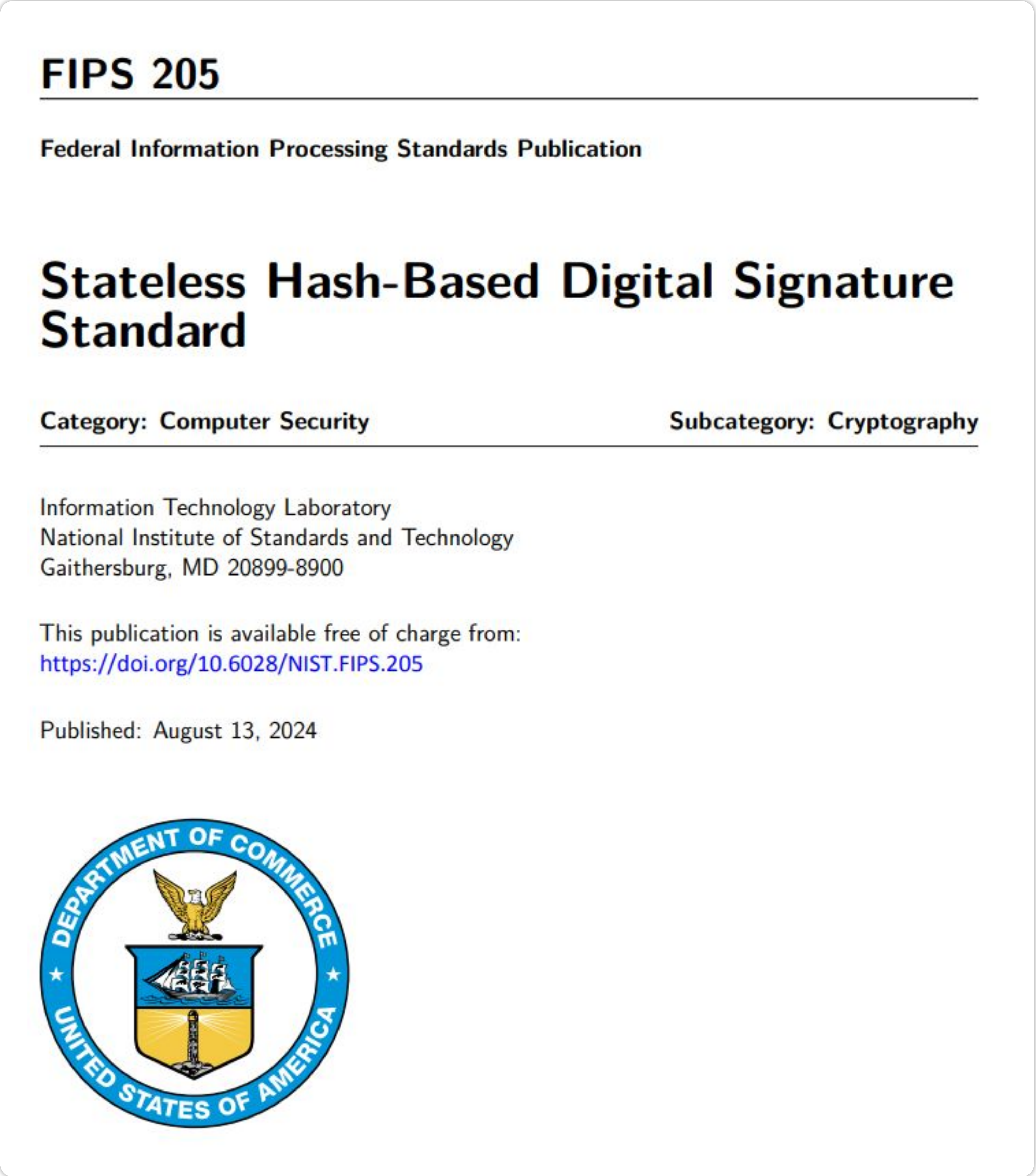
| | |
|---|---|
| Fall 2016 | Formal Call for Proposals |
| Nov 2017 | Deadline for submissions |
| Early 2018 | Workshop - Submitter's Presentations |
| 3-5 years | Analysis Phase - NIST will report findings<br>*1-2 workshops during this phase* |
| 2 years later | Draft Standards ready |

# NIST standards and round 4

Standards announced in 2022:

- Encryption/KEM: **Kyber** (ML-KEM, FIPS 203)
- Signature:
  - **Dilithium** (ML-DSA, FIPS 204)
  - **SPHINCS+** (SLH-DSA, FIPS 205)
  - **Falcon** (*TBD*)

All *latticed-based* except SPHINCS+


FIPS 205

Federal Information Processing Standards Publication

Stateless Hash-Based Digital Signature Standard

Category: Computer Security — Subcategory: Cryptography

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.205

Published: August 13, 2024



**Round 4** only for encryption/KEM, all *code-based*:

~~BIKE, Classic McEliece~~, **HQC** selected as the winner in 2025

# Lattice-based crypto intuition

Based on problems such as **learning with errors** (LWE):

**S** a secret vector of numbers

The attacker receives pairs of vectors (**A**, **B**)

- **A** = ($A_0$, …, $A_{n-1}$) is a vector of uniformly random numbers
- **B** = <**S**, **A**> + **E** , a vector of $B_i$ = $S_i$*$A_i$ + $E_i$
- **E** = ($E_0$, …, $E_{n-1}$) is an **unknown** vector or *normal*-random numbers

Attacker's goal: find **S** given many pairs (**A**, **B**)

# Lattice-based crypto intuition

Based on problems such as **learning with errors** (LWE):

**S** a secret vector of numbers

The attacker receives pairs of vectors (**A**, **B**)

- **A** = ($A_0$, …, $A_{n-1}$) is a vector of uniformly random numbers
- **B** = <**S**, **A**> + **E** , a vector of $B_i$ = $S_i$*$A_i$ + $E_i$
- **E** = ($E_0$, …, $E_{n-1}$) is an **unknown** vector or *normal*-random numbers

Attacker's goal: find **S** given many pairs (**A**, **B**)

Without the errors **E**: trivial to solve (just a linear systems of equations)

With the errors **E**: **NP-hard**

# PQC performance

| Algorithm | Public key (bytes) | Ciphertext (bytes) | Key gen. (ms) | Encaps. (ms) | Decaps. (ms) | |
|---|---|---|---|---|---|---|
| ECDH NIST P-256 | 64 | 64 | 0.072 | 0.072 | 0.072 | Elliptic curve key agreement |
| SIKE p434 | 330 | 346 | 13.763 | 22.120 | 23.734 | |
| Kyber512-90s | 800 | 736 | 0.007 | 0.009 | 0.006 | Post-quantum standard |

| Algorithm | Public key (bytes) | Signature (bytes) | Sign (ms) | Verify (ms) | |
|---|---|---|---|---|---|
| ECDSA NIST P-256 | 64 | 64 | 0.031 | 0.096 | Elliptic curve signature |
| Dilithium2 | 1,184 | 2,044 | 0.050 | 0.036 | Post-quantum standard |

From "Benchmarking Post-Quantum Cryptography in TLS" https://eprint.iacr.org/2019/1447

# Using PQC today

Integrated by most **hyperscalers**

## Cloudflare now uses post-quantum cryptography to talk to your origin server

2023-09-29

AWS Security Blog

## Post-quantum TLS now supported in AWS KMS

by Andrew Hopkins | on 04 NOV 2019 | in Advanced (300), AWS Key Management Service, Security, Identity, & Compliance | Permalink | Comments | Share

Security & Identity

## Announcing quantum-safe digital signatures in Cloud KMS

February 21, 2025

**Software libraries**

## OpenSSL 3.5.0 now contains post-quantum procedures

With the new LTS version 3.5.0, OpenSSL adds the post-quantum methods ML-KEM, ML-DSA and SLH-DSA to its library.

open-quantum-safe / **liboqs**

<> Code | Issues 19 | Pull requests 4 | Actions | Projects 0 | W

C library for quantum-safe cryptography. https://openquantumsafe.org/

mupq / **pqm4**

<> Code | Issues 3 | Pull requests 0 | Actions

Post-quantum crypto library for the ARM Cortex-M4

# More about post-quantum crypto

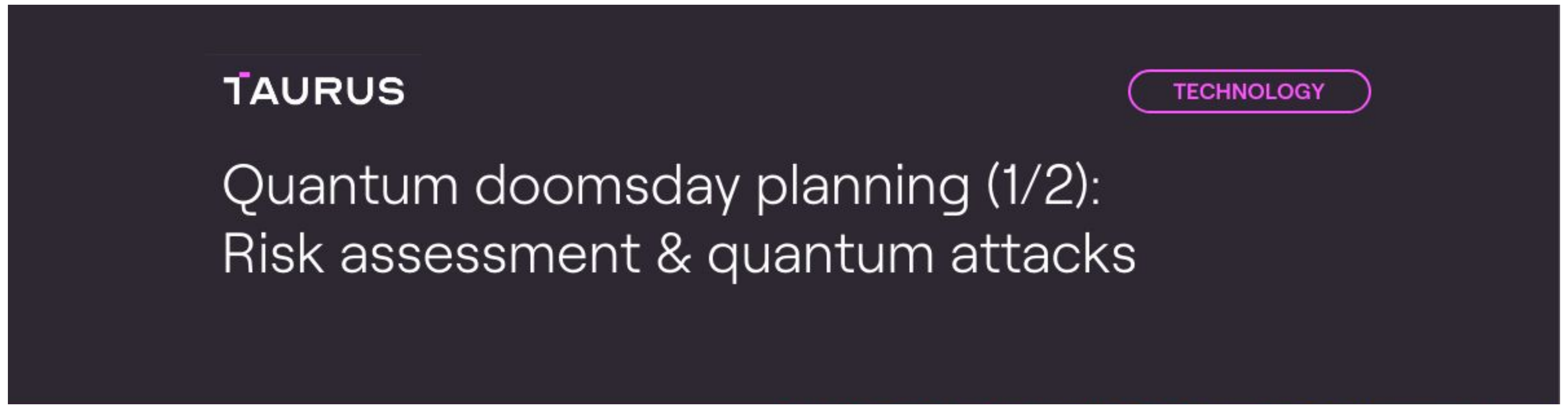
https://github.com/veorq/awesome-post-quantum

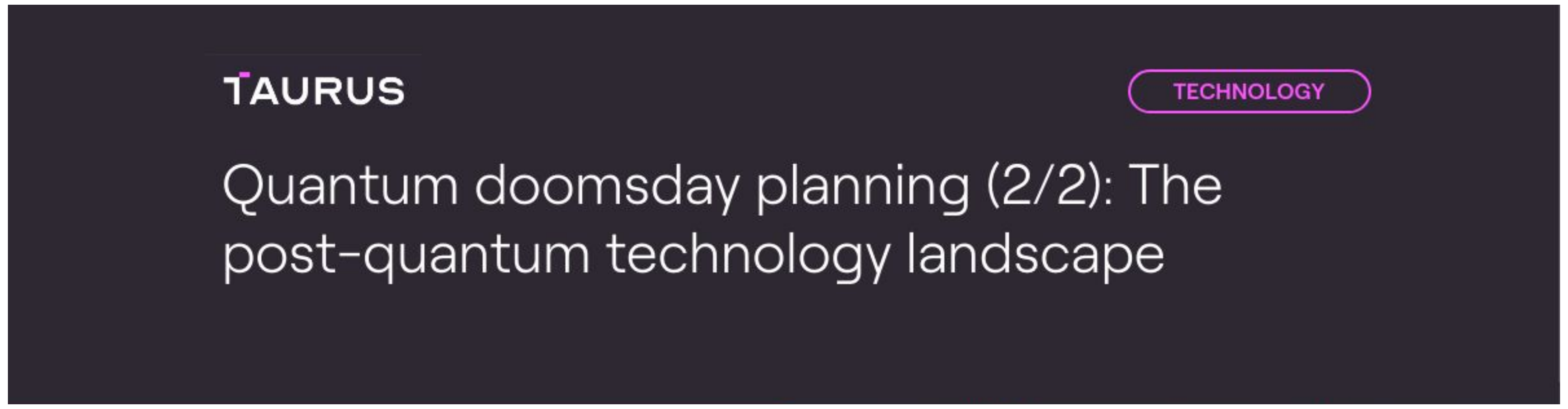
https://github.com/qosf/awesome-quantum-software

https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

IETF RFC 8391 (XMSS), RFC 8554 (LM)

May 2023 articles on https://blog.taurushq.com/, on how to prepare for the transition in an enterprise IT environment (inventory, risk management, etc.)



TAURUS

شكرًا جزيلاً

# شكرًا جزيلاً

# Thank you!

jp@taurushq.com