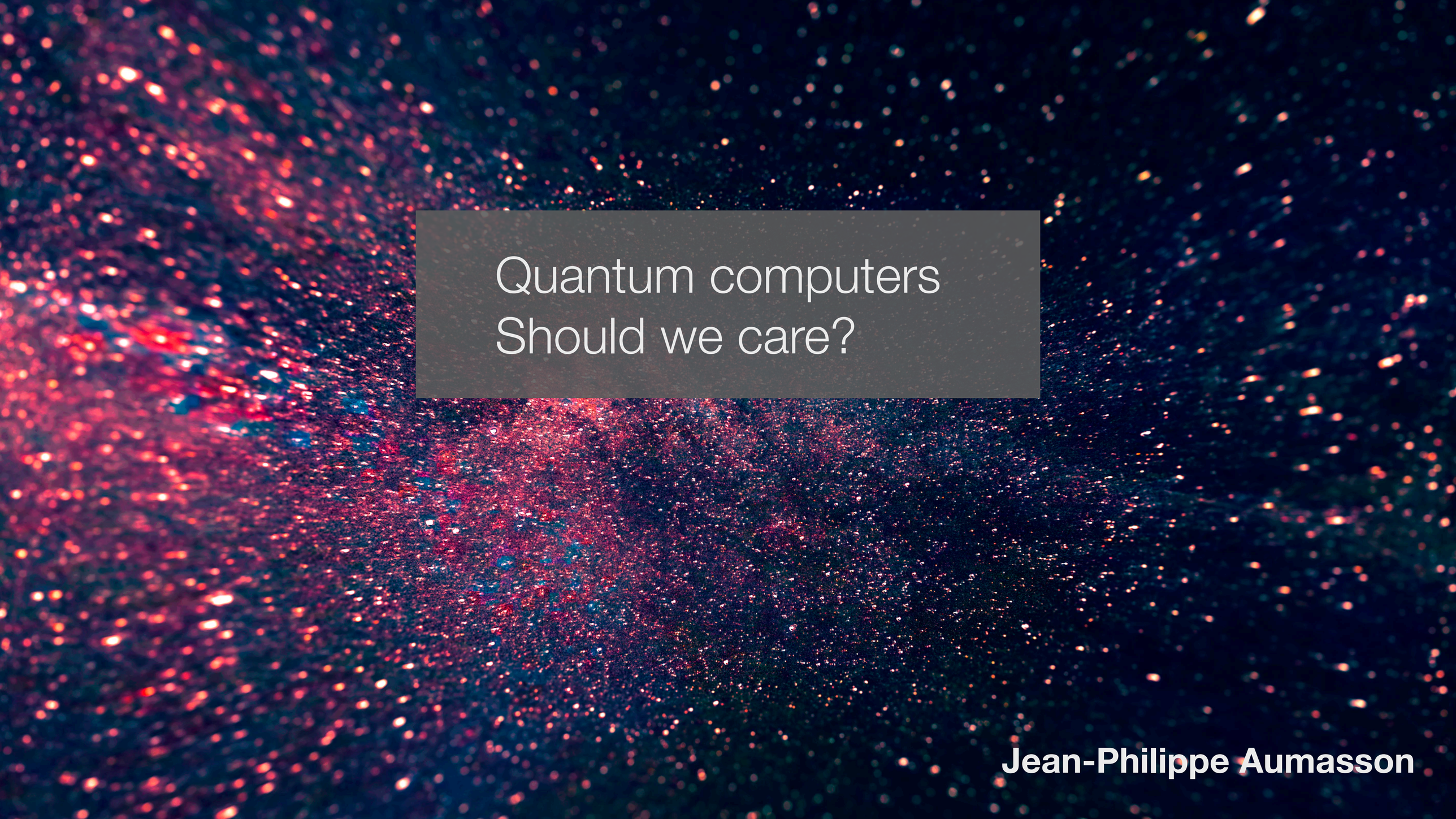

Quantum computers
Should we care?
Jean-Philippe Aumasson

/me

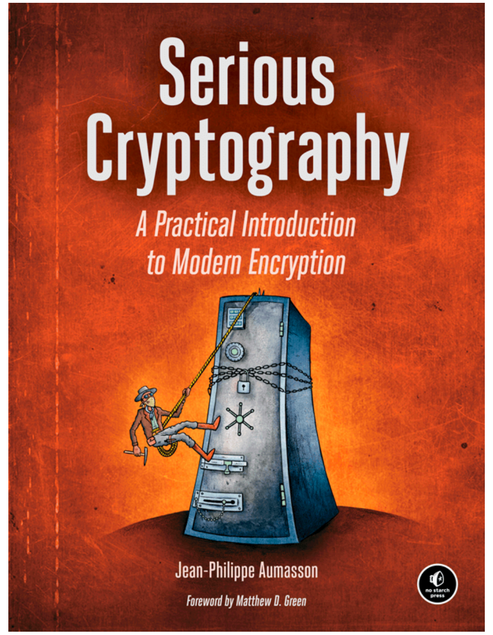
Cryptography expert, in crypto/security for 13 years, EPFL PhD

Designed popular algorithms, researched **post-quantum** crypto

Currently:

- **Founder** of Teserakt AG, IoT end-to-end security
- **Security head** at Taurus Group, fintech /digital assets
- **VP** at Kudelski Security, research and security audits

https://aumasson.jp



Simulating Physics with Computers

Richard P. Feynman

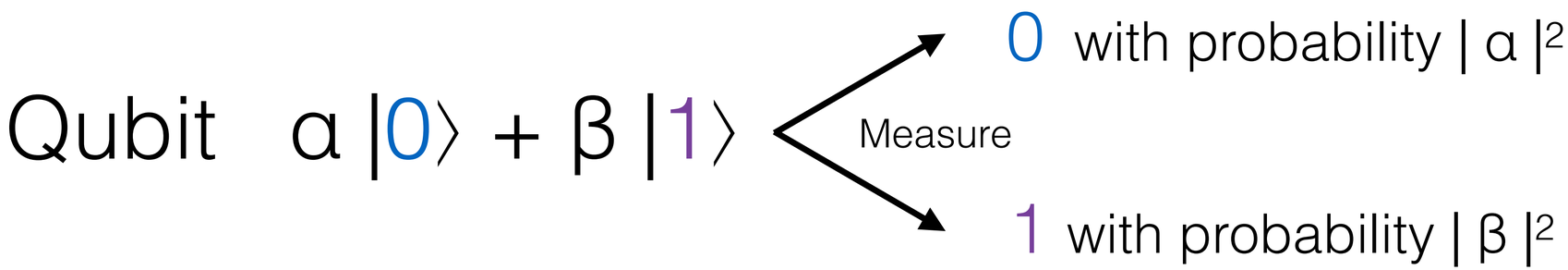
Department of Physics, California Institute of Technology, Pasadena, California 91107

Received May 7, 1981

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

Qubits instead of bits



Stay 0 or 1 forever

Generalizes to more than 2 states: qutrits, qubytes, etc.

Complex, negative probabilities (amplitudes), **real randomness**

Quantum computer

Just high-school linear algebra

Quantum registers, a bunch of quantum states

~ N qubits encode a list of 2^N amplitudes

Quantum assembly instructions

~ Matrix multiplications preserving amplitudes' normalization

Quantum circuits usually end with a **measurement**

Can’t be simulated classically! (needs 2^N storage/compute)

Quantum speedup

A quantum computer does **not run faster** than a classical one

—it's not about speed of computation

Instead they can solve **very specific problems** using a lower complexity, for example $O(n^3)$ instead of $O(2^n)$

Most interesting: **exponential** quantum speedup

Quantum parallelism

Quantum computers sort of encode all values simultaneously

But they **do not “try every answer in parallel”**

You can only observe one result, and can’t select “the best”

Quantum vs. crypto problems

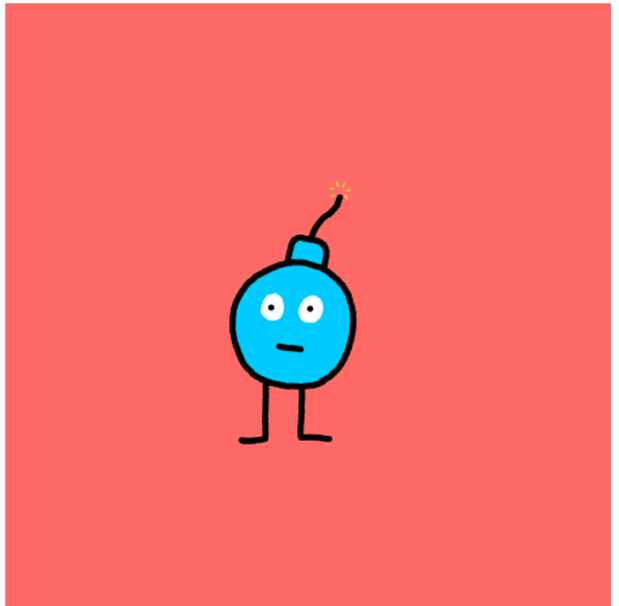
Shor's quantum algorithm solves these problems efficiently:

- Finds **p** given **n** = **pq** (= **factoring** problem)
- Finds **d** given **y** = $\mathbf{x}^{\mathbf{d}}$ mod **p** (= **discrete log** problem)

Fast on a quantum computer

Practically impossible classically

#ExponentialSpeedup



How bad is it?

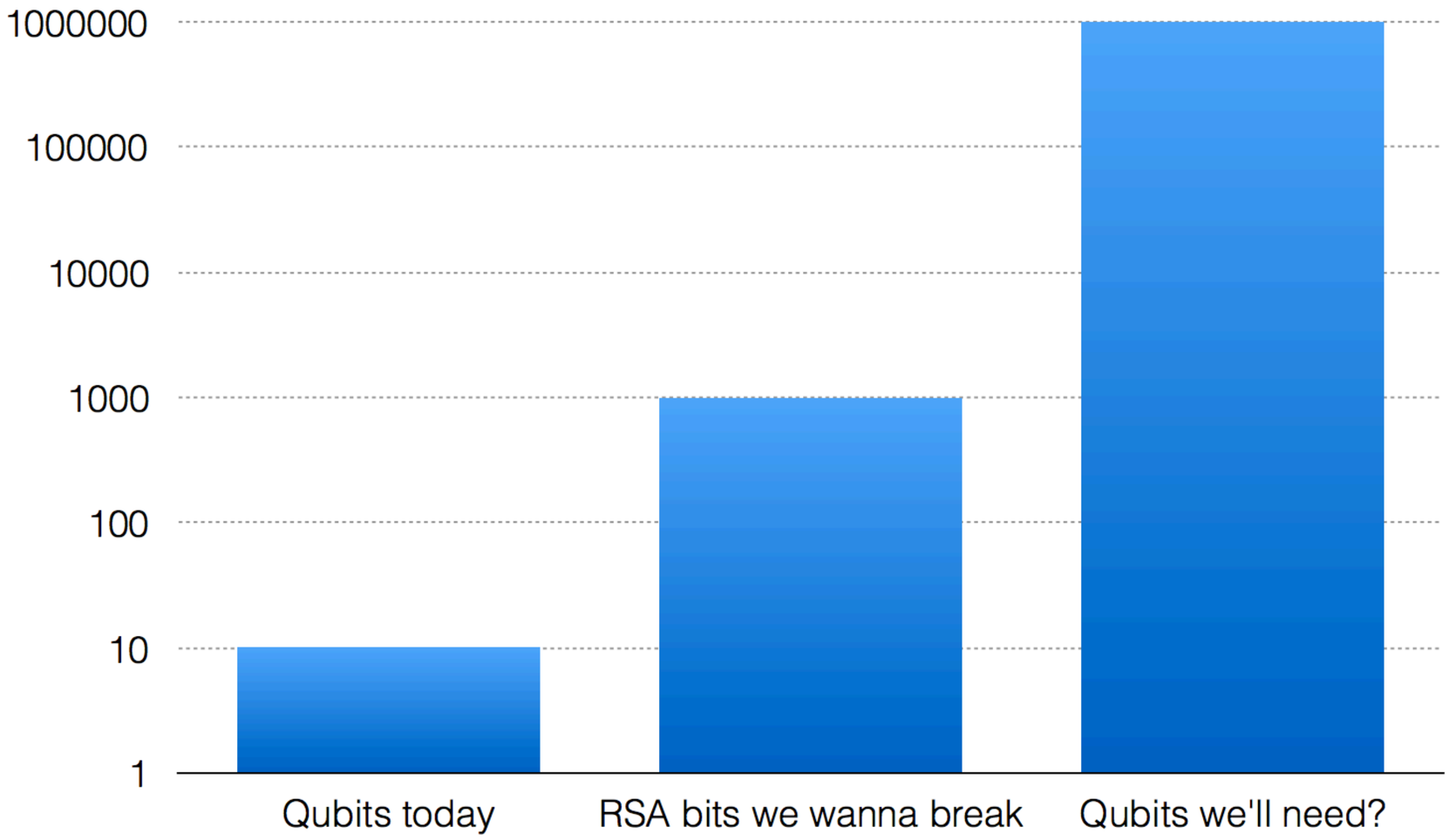
All public-key cryptosystem broken 😱
(RSA, Diffie-Hellman, elliptic curves)

Therefore, all security broken (web, mobile, infrastructure, etc.)

- TLS, PKI-based authentication systems, certificate pinning
- SSH, IPsec, most VPN software

Exception: symmetric-key only systems like Kerberos, pre-shared key TLS, 4G/5G authentication/encryption, etc.

We’re not there yet



(log scale)

Quantum vs. AES

NIST's "**Advanced Encryption Standard**"

- THE symmetric encryption standard
- Supports keys of 128, 192, or 256 bits
- **Everywhere**: TLS, SSH, IPsec, quantum links, etc.

Quantum search

Grover's algorithm: searches in N items in $\sqrt{N}$ queries!

=> AES broken in $\sqrt{(2^{128})} = 2^{64}$ operations

Caveats behind this simplistic view:

- It's actually **$O(\sqrt{N})$**, constant factor in O()'s may be huge
- Doesn't easily parallelize as classical search does

Grover is not a problem, just double key length

And that’s it, problem solved!

Defeating quantum computing

Post-quantum crypto

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

Algorithms not broken by a quantum computer…

- Must not rely on factoring or discrete log problems
- Must be well-understood with respect to quantum

Why care?

Insurance against QC threat:

- “QC has a probability *p* work in year 2YYY”
- “I’d like to eliminate this risk”

NSA recommendations for National Security Systems

"we anticipate a need to shift to quantum-resistant cryptography in the near future.”

(In CNSS advisory 02-15)

NIST standardization

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 *1-2 workshops during this phase*
2 years later	Draft Standards ready

Conclusions

- Quantum computer would break all public-key crypto
- Unlikely before at least 30 years, if ever (***my*** perspective)
- **Post-quantum** crypto is a replacement safe against quantum computers, expect NIST standards in 2022
- Recommended reading: