Towards post-quantum crypto standards

Jean-Philippe Aumasson

Teserakt

Fundamental Equations

Schrödinger equation:

$$i\hbar\frac{\partial\Psi}{\partial t} = H\Psi$$

Time independent Schrödinger equation:

$$H\psi = E\psi, \qquad \Psi = \psi e^{-iEt/\hbar}$$

Standard Hamiltonian:

$$H = -\frac{\hbar^2}{2m}\nabla^2 + V$$

Time dependence of an expectation value:

$$\frac{d\langle Q\rangle}{dt} = \frac{i}{\hbar}\langle[H,Q]\rangle + \left\langle\frac{\partial Q}{\partial t}\right\rangle$$

Generalized uncertainty principle:

$$\sigma_A\sigma_B \geq \left|\frac{1}{2i}\langle[A,B]\rangle\right|^2$$

Simulating Physics with Computers

Richard P. Feynman

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

Received May 7, 1981

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

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

Qubit $\alpha\,|0\rangle + \beta\,|1\rangle \xrightarrow{\text{Measure}}$

0 with probability $|\,\alpha\,|^2$

1 with probability $|\,\beta\,|^2$

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

When quantum computers can solve a problem faster than classical computers

Most interesting: **Superpolynomial** quantum speedup

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

Quantum parallelism

Quantum computers sort of encode all values simultaneously

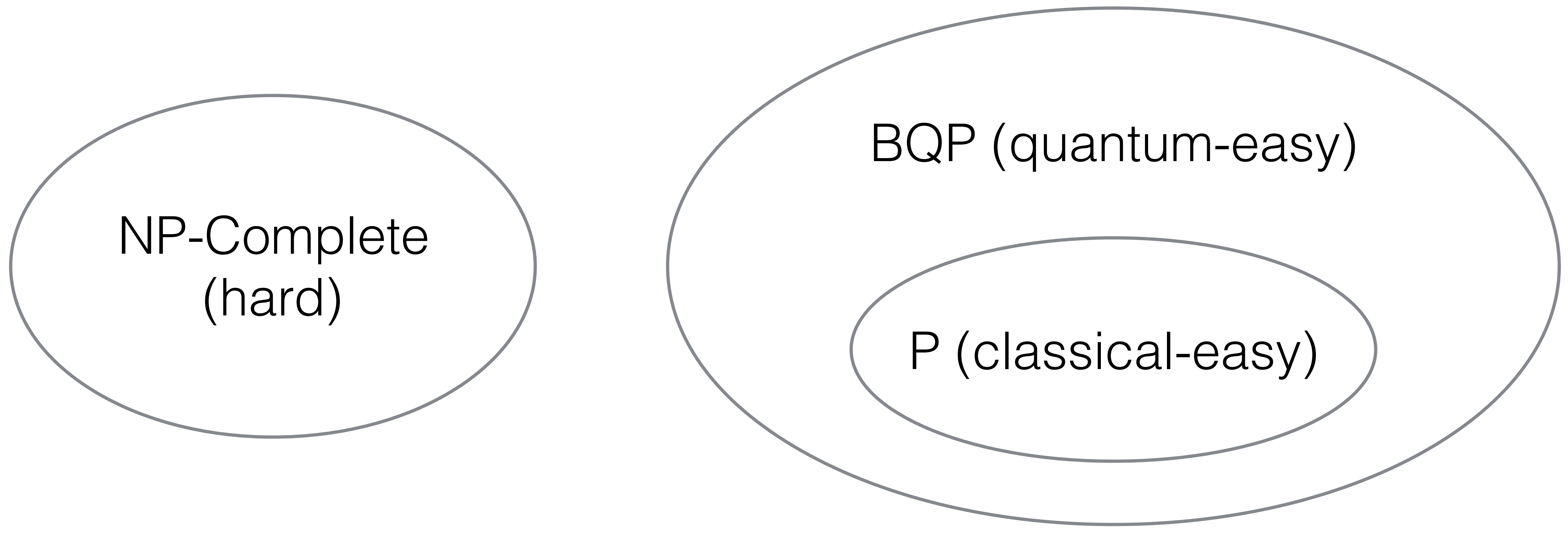
But they do not “try every answer in parallel”

You can only observe one result, not all

NP-complete problems

- Solution hard to find, but easy to verify
- SAT, scheduling, Candy Crush, etc.
- Sometimes used in crypto

Can't be solved faster with quantum computers (so we believe)



Intelligent Machines

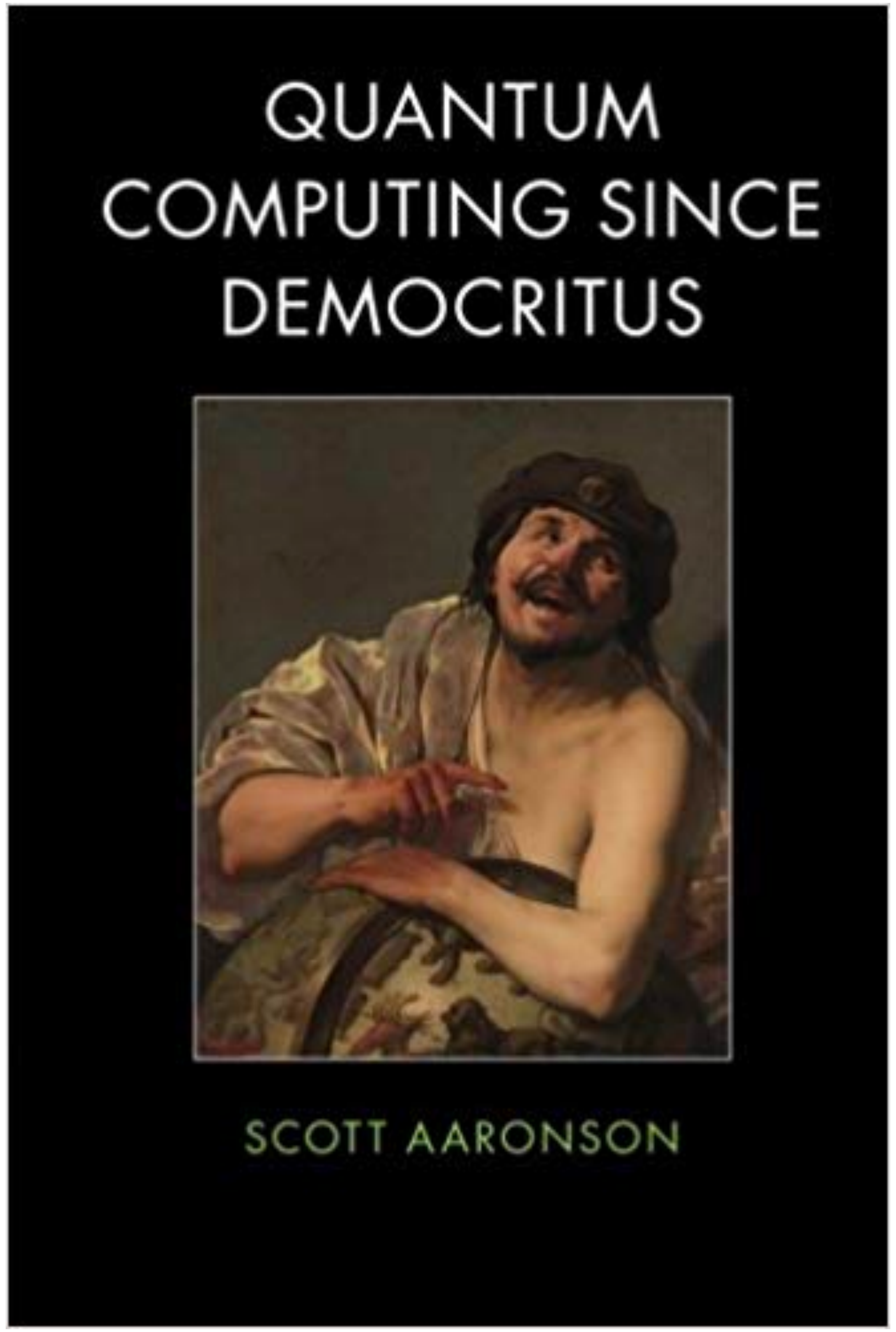
Google thinks it's close to "quantum supremacy." Here's what that really means.

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

Recommended



How broken are your public keys?

Shor them all

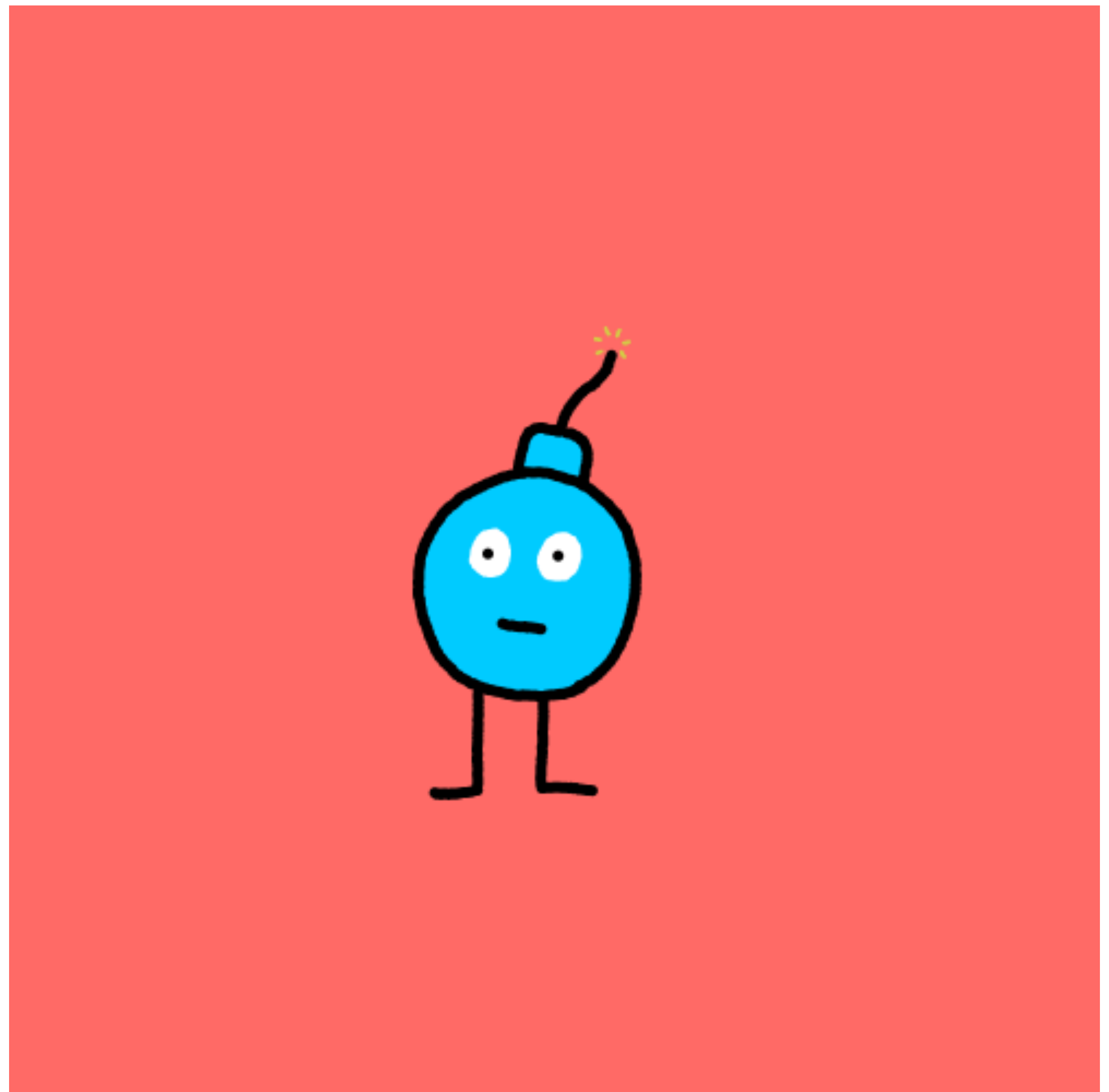
Shor's algorithm finds a structure in abelian subgroups:

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

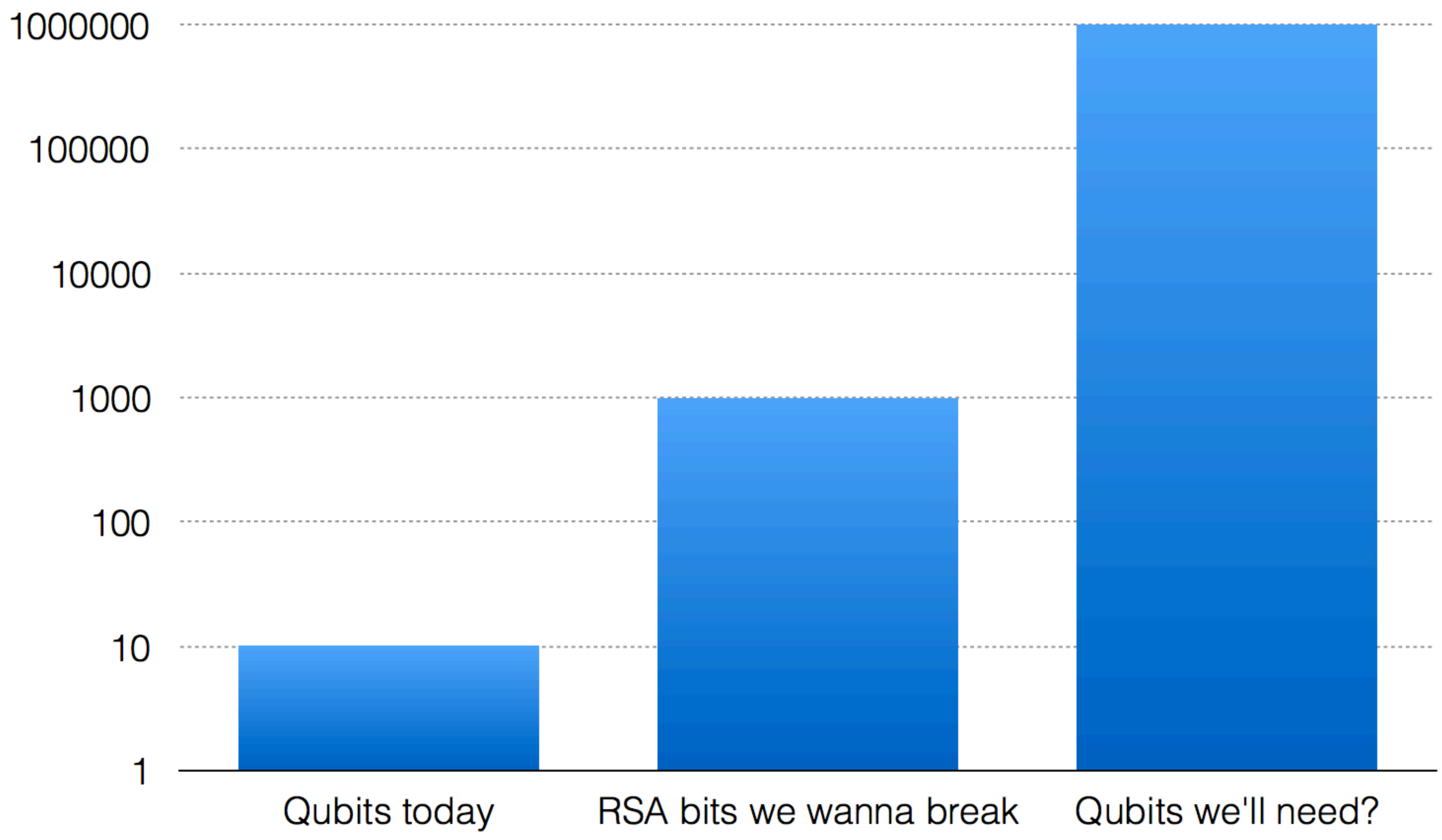
Fast on a quantum computer

Practically impossible classically

#ExponentialSpeedup



We’re not there yet



(log scale)

Designing a Million-Qubit Quantum Computer Using Resource Performance Simulator

Muhammad Ahsan, Rodney Van Meter, Jungsang Kim

(Submitted on 2 Dec 2015)

The optimal design of a fault-tolerant quantum computer involves finding an appropriate balance between the burden of large-scale integration of noisy components and the load of improving the reliability of hardware technology. This balance can be evaluated by quantitatively modeling the execution of quantum logic operations on a realistic quantum hardware containing limited computational resources. In this work, we report a complete performance simulation software tool capable of (1) searching the hardware design space by varying resource architecture and technology parameters, (2) synthesizing and scheduling fault-tolerant quantum algorithm within the hardware constraints, (3) quantifying the performance metrics such as the execution time and the failure probability of the algorithm, and (4) analyzing the breakdown of these metrics to highlight the performance bottlenecks and visualizing resource utilization to evaluate the adequacy of the chosen design. Using this tool we investigate a vast design space for implementing key building blocks of Shor's algorithm to factor a 1,024-bit number with a baseline budget of 1.5 million qubits. We show that a trapped-ion quantum computer designed with twice as many qubits and one-tenth of the baseline infidelity of the communication channel can factor a 2,048-bit integer in less than five months.

AES vs. quantum search

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

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 worth less than 5 grams of hydrogen)

No doubts more efficient circuits will be designed…

Grover is not a problem…

… just double key length

And that’s it, problem solved!

Defeating quantum computing

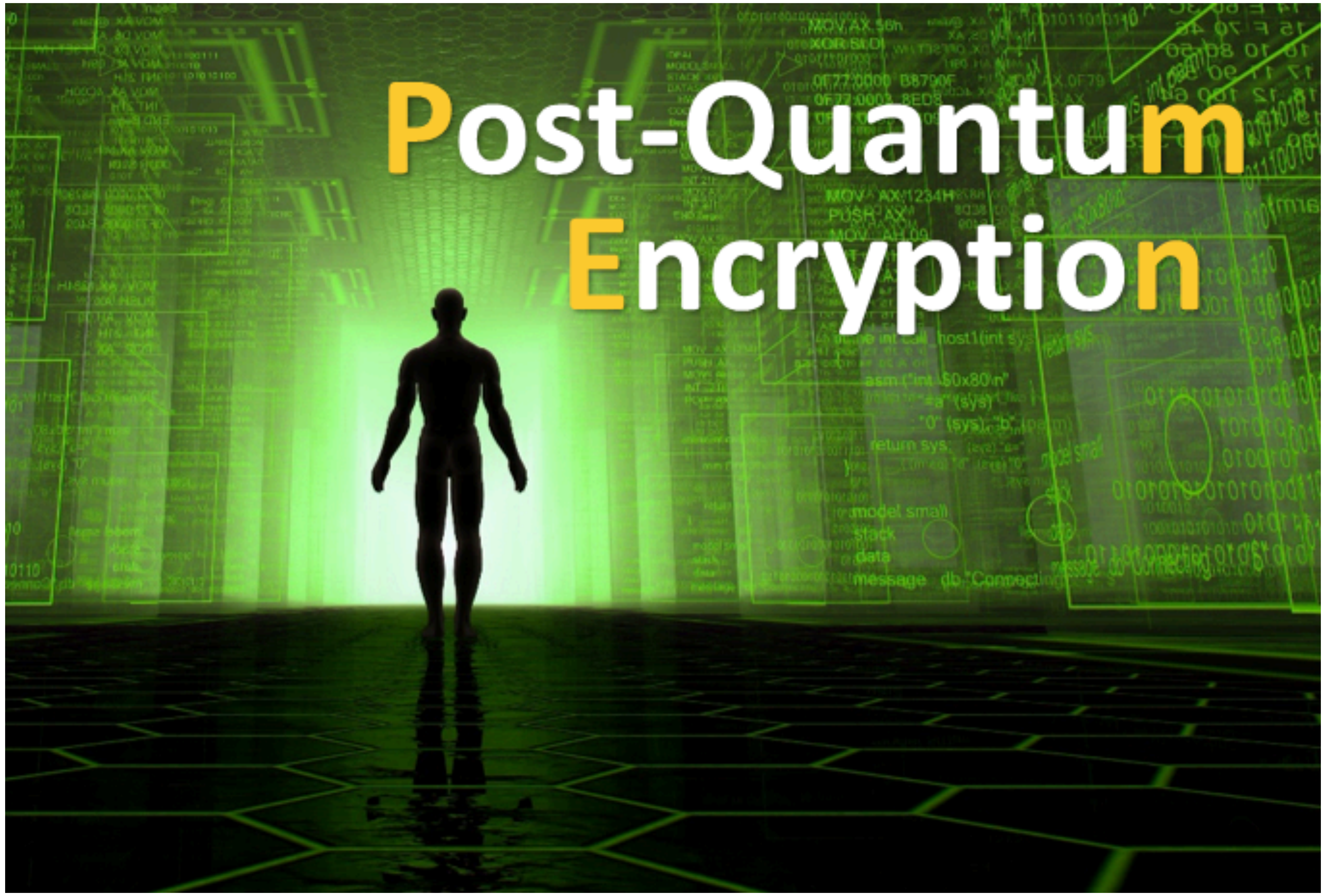


Image credit: company Dyadic Security

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

Have sometimes been broken.. classically ¯_(ツ)_/¯

Why care?

Insurance against QC threat:

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

Why care?

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)

Why care?

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

NIST's project

FINAL SUBMISSIONS RECEIVED

- The deadline is past – no more submissions
- 82 total submissions received
  - 23 signature schemes
  - 59 Encryption/KEM schemes

	Signatures	KEM/Encryption	Overall
Lattice-based	4	24	28
Code-based	5	19	24
Multi-variate	7	6	13
Hash-based	4		4
Other	3	10	13
Total	**23**	**59**	**82**

See https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

Lattice-based crypto

TECHNOLOGY

Google Experimenting With 'New Hope' Post-Quantum Encryption To Safeguard Chrome

Google Security Blog

The latest news and insights from Google on security and safety on the Internet

Experimenting with Post-Quantum Cryptography

July 7, 2016

Lattice-based crypto

Google's Post-Quantum Cryptography

News has been bubbling about an announcement by Google that it's starting to experiment with public-key cryptography that's resistant to cryptanalysis by a quantum computer. Specifically, it's experimenting with the New Hope algorithm.

It's certainly interesting that Google is thinking about this, and probably okay that it's available in the Canary version of Chrome, but this algorithm is by no means ready for operational use. Secure public-key algorithms are *very* hard to create, and this one has not had nearly enough analysis to be trusted. Lattice-based public-key cryptosystems such as New Hope are particularly subtle -- and we cryptographers are still learning a lot about how they can be broken.

Targets are important in cryptography, and Google has turned New Hope into a good one. Consider this an opportunity to advance our cryptographic knowledge, not an offer of a more-secure encryption option. And this is the right time for this area of research, before quantum computers make discrete-logarithm and factoring algorithms obsolete.

More post-quantum families

- Based on **coding theory** (McEliece, Niederreiter):
  - Solid foundations (late 1970s)
  - Large keys (dozen kBs)
  - *Encryption only*
- Based on **multivariate polynomials** evaluation
  - Secure in theory, not always in practice
  - *Mostly for signatures*

Hash functions are post-quantum!

Hash functions

- Input of any size, output of 256 or 512 bits
- Can't invert, can't find collisions
- BLAKE2, SHA-3, SHA-256, ~~SHA-1~~, ~~MD5~~…

Hash-based signatures

Unique compared to other post-quantum schemes:

- No mathematical/structured hard problem
- As secure as underlying hash functions
- Good news: we have secure hash functions!

Hash-based signatures

But there’s a catch…

Hash-based signatures

- Not fast (but not always a problem)
- Large signatures (dozen of kBs)
- Statefulness problem…

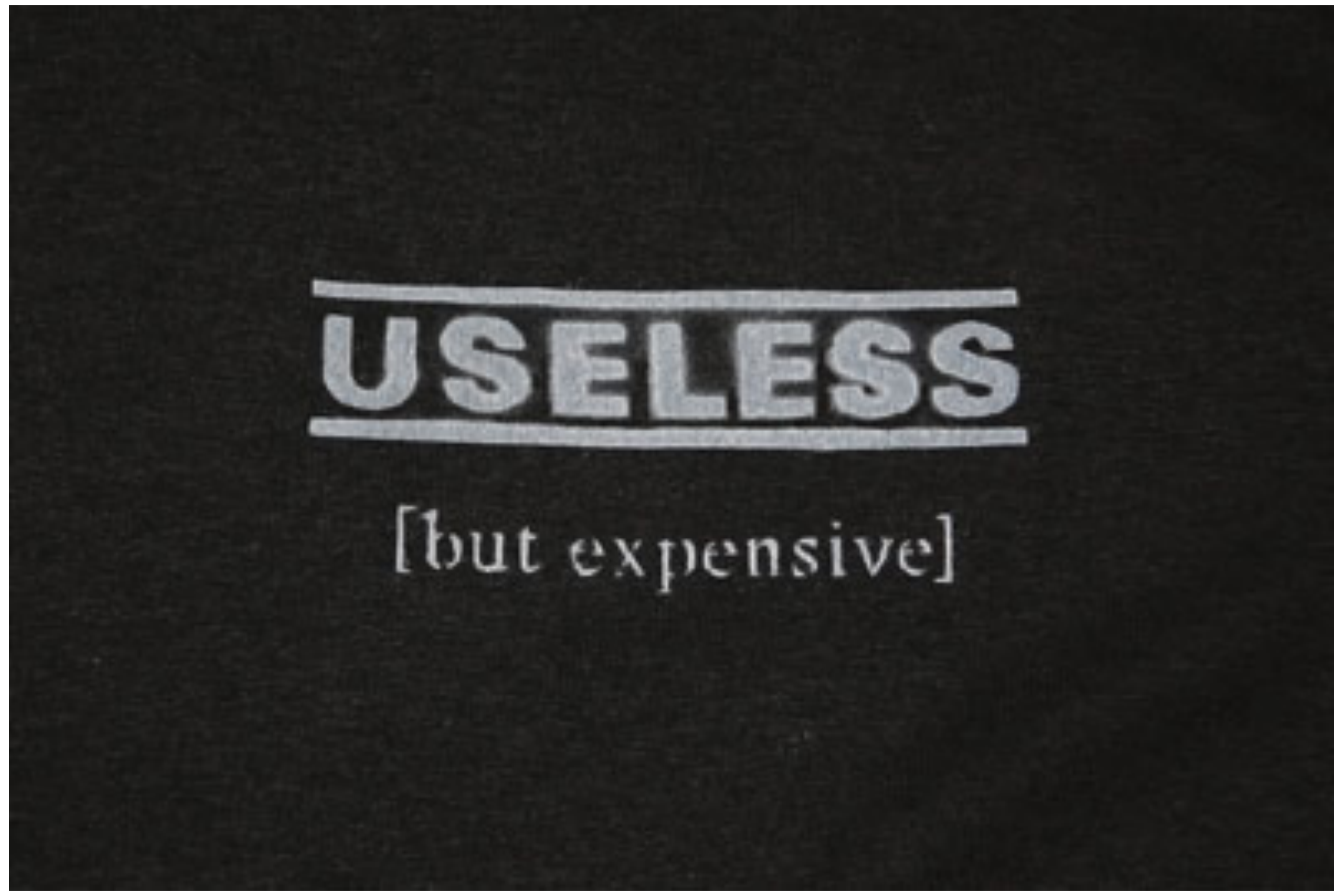
One-time signatures

Lamport, **1979**:

1. Generate a key pair
   - Pick random strings $\mathbf{K}_0$ and $\mathbf{K}_1$ (your **private key**)
   - The public key is the two values $\mathbf{H}(\mathbf{K}_0)$, $\mathbf{H}(\mathbf{K}_1)$

2. To sign the bit 0, show $\mathbf{K}_0$, to sign 1 show $\mathbf{K}_1$

One-time signatures



- Need as many keys as there are bits
- A key can only be used once

Sign more than 0 and 1

Winternitz, **1979**:

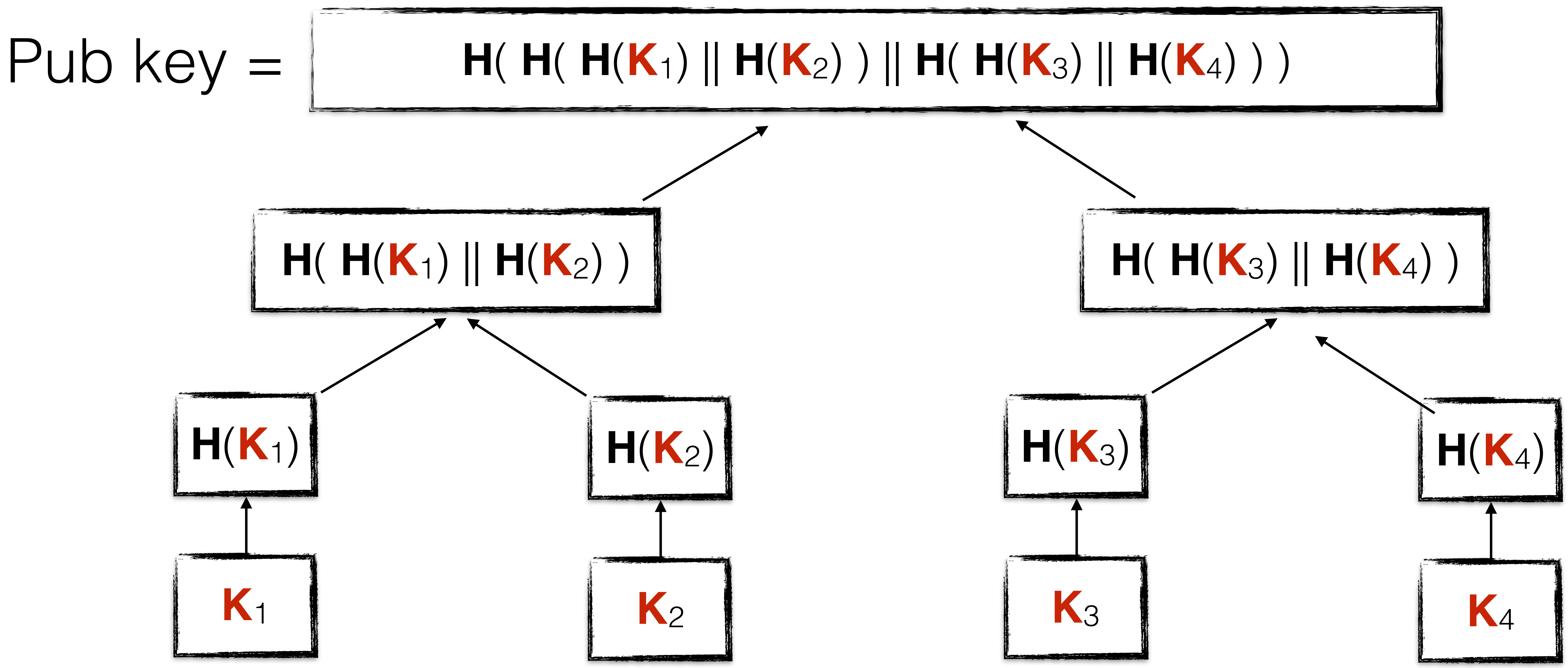
1. Public key is $\mathbf{H}(\mathbf{H}(\mathbf{H}(\mathbf{H}(\ldots. (\mathbf{K})\ldots)) = \mathbf{H}^{\mathbf{w}}(\mathbf{K})$. ($\mathbf{w}$ times)
2. To sign a number $\mathbf{x}$ in $[0; \mathbf{w} - 1]$, compute $\mathbf{S}=\mathbf{H}^{\mathbf{x}}(\mathbf{K})$

Verification: check that $\mathbf{H}^{\mathbf{w-x}}(\mathbf{S})$ = public key

A key must still be used only once

From one-time to many-time

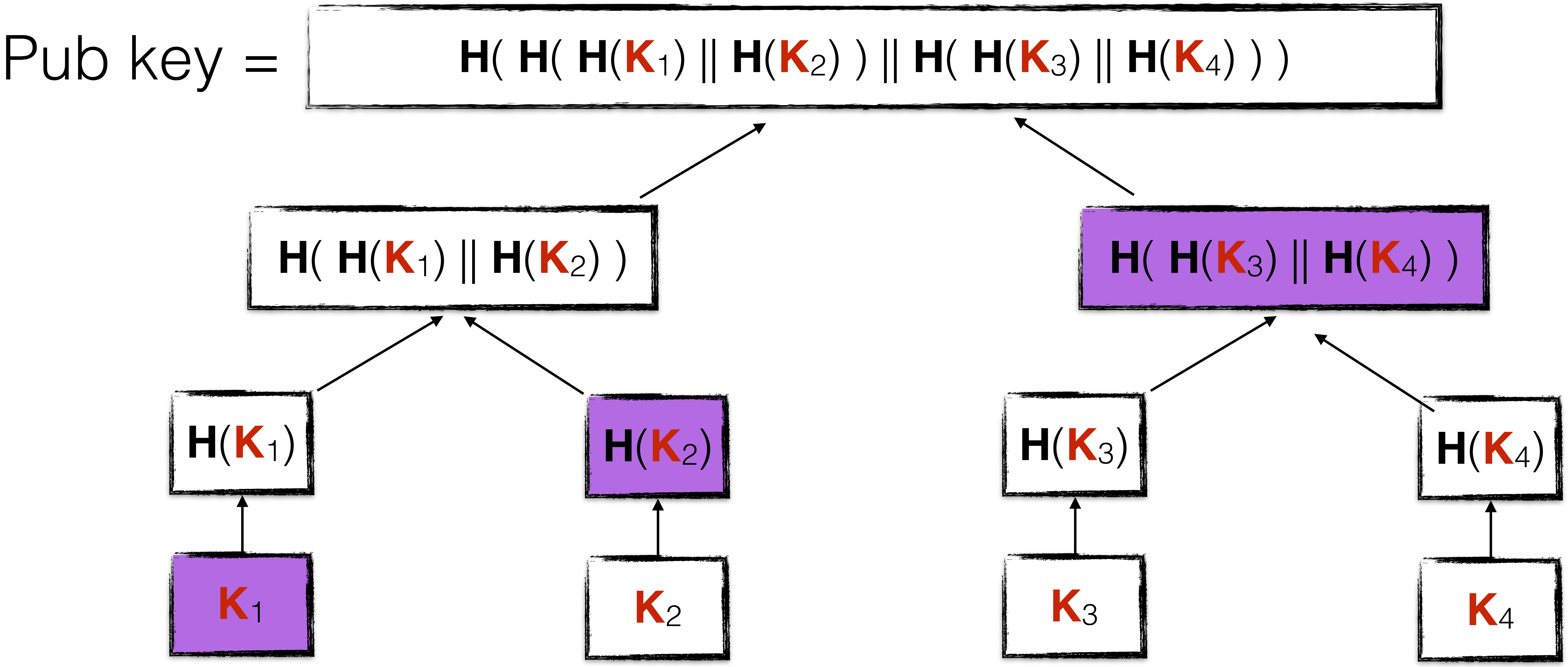
"Compress" a list of one-time keys using a **hash tree**



From one-time to many-time

When a new **one-time public key** K_i, is used…

… give its **authentication path** to the root pub key



Conclusion

When/if a scalable and quantum computer is built…

- Public keys could be broken after some effort…
- Symmetric-key security will be at most halved

Post-quantum crypto..

- Would not be defeated by quantum computers
- Post-quantum crypto NIST competition starting..
  - All submissions and their code are public
  - Standardized algorithm available in a few years