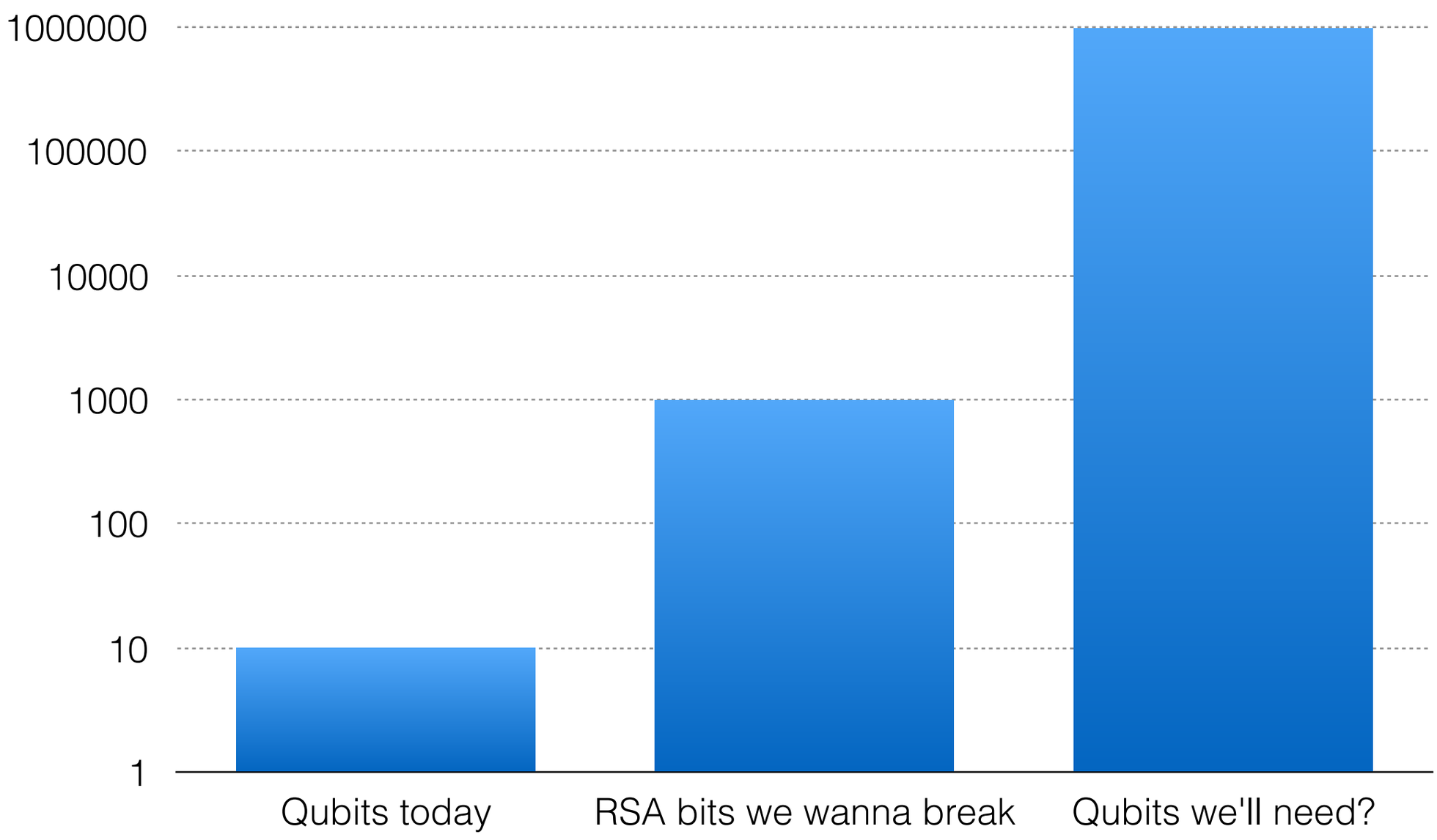
Crypto, Quantum, Post-Quantum

JP Aumasson / @veorq, Kudelski Security, Switzerland

We’re not there yet



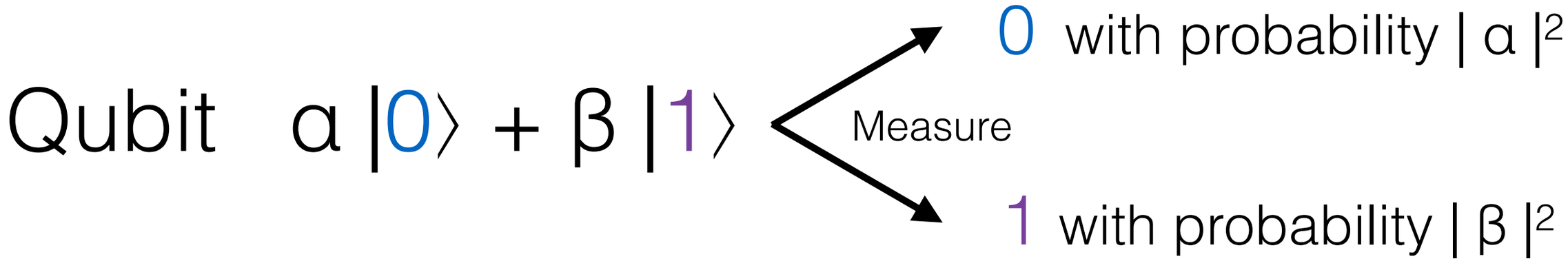
Hillary Clinton wants “Manhattan-like project” to break encryption

US should be able to bypass encryption—but only for terrorists, candidate says.

by **Jon Brodkin** - Dec 21, 2015 5:15pm CET

Such bombs might very well prove to be too heavy for transportation by air. —Albert Einstein, 1939

Just random 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

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/

Killer application

Factoring and solving discrete logs

- Both "Abelian hidden subgroup problems”
- Superpolynomial speedup! $O(2^{n/3})$ -> $O(n^3)$ for factoring

RIP RSA ECC DH; PGP SSH TLS OTR Axolotl Tor Bitcoin …

Not impacted: 3G–4G/LTE WPA2 Kerberos

Breaking RSA-2048 would take **months** and million qubits

(from http://arxiv.org/abs/1512.00796)

Impact for symmetric crypto

Polynomial speedup thanks to **Grover's search** algorithm

Search among 2^n unsorted values in time $O(2^{n/2})$ instead of $O(2^n)$

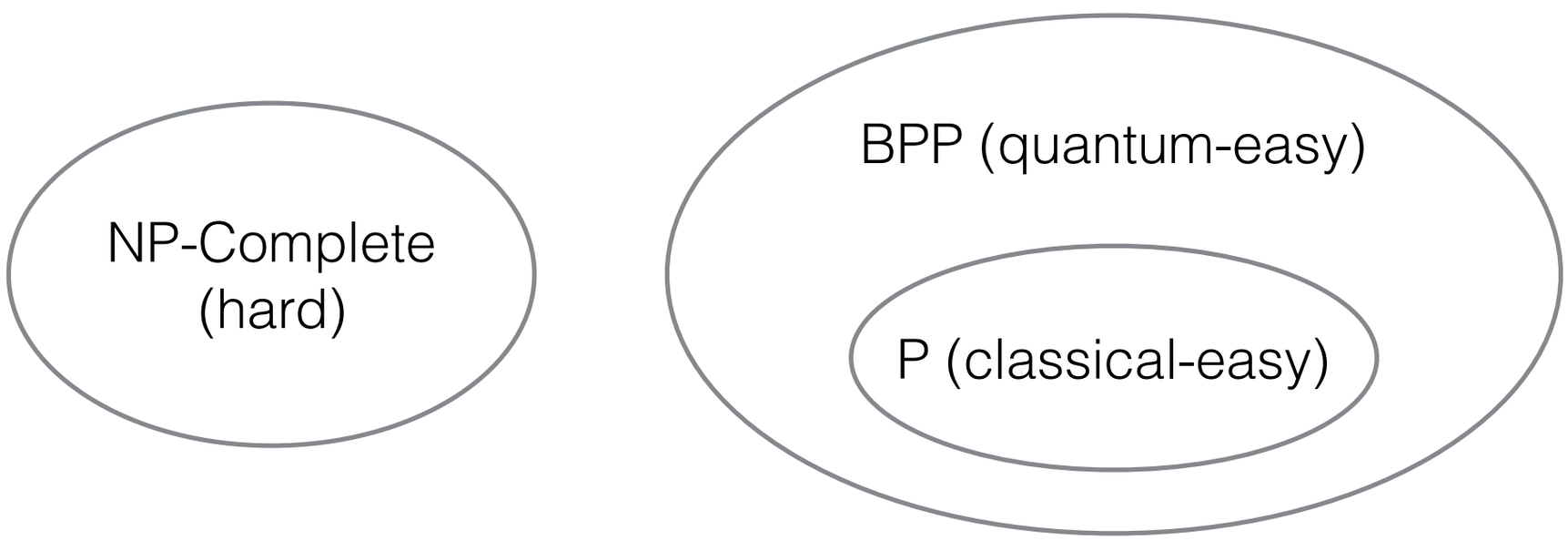
- AES-128 security downgraded from 128 to 64 bits
- SHA-256 preimage security downgraded from 256 to 128 bits
- Doesn't really help for finding collisions

Solution: double key/hash length

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)



Post-quantum crypto

Public-key crypto **probably not broken** by a quantum computer

- A.k.a. quantum-safe, quantum-resistant crypto
- NP-hardness tempting, but hard to leverage for crypto

A hot thing these days (seen on Wired, etc.)

NATALIE WOLCHOVER SCIENCE 09.19.15 7:00 AM

THE TRICKY ENCRYPTION THAT COULD STUMP QUANTUM COMPUTERS

Because, NSA

In August 2015, NSA said it wants to post-quantum Suite B

“Not too distant future”: Expect at least 10 years before a standard, at least 25 years before wide adoption

Koblitz/Menezes theories

“NSA can break post-quantum crypto“ (and wants you to use it)

“NSA can break RSA” (and wants to delay move to ECC)

“NSA was thinking of gov users” (who take ages to switch crypto)

“NSA believes RSA-3072 is much more quantum-resistant than ECC-256 and even ECC-384“

“NSA is using a diversion strategy aimed at Russia and China"

“NSA has a political need to distance itself from ECC"

Should we care?

Risk management as usual

- Quantum computers may or may not show up
- I believe not before 100 years, but others say 10 years
- What insurance price are you ready to pay?

High-impact for **encryption**: all previous ciphertexts compromised

Not so much for **signatures**, if you can later revoke pre-quantum keys and issue fresh post-quantum signatures if needed

What can we do now?

http://pqcrypto.eu.org/ already issued “Initial recommendations”

- Code-based encryption (McEliece)
- Hash-based signatures (XMSS, SPHINCS)

PQCRYPTO

Post-Quantum Cryptography for Long-Term Security

Project number: Horizon 2020 ICT-645622

Initial recommendations of long-term secure post-quantum systems

Hash-based signatures

As strong as the underlying hash function's preimage security

SPHINCS, by DJB and others http://sphincs.cr.yp.to/

- 41KB signatures, 1KB keys, 100s signatures/second

SPHINCS: practical stateless hash-based signatures

Introduction | Papers | Software

The following paper introduces the HORST few-time signature scheme, the SPHINCS many-time signature scheme, and SPHINCS-256:

XMSS, by Buchmann and others, now an Internet-Draft

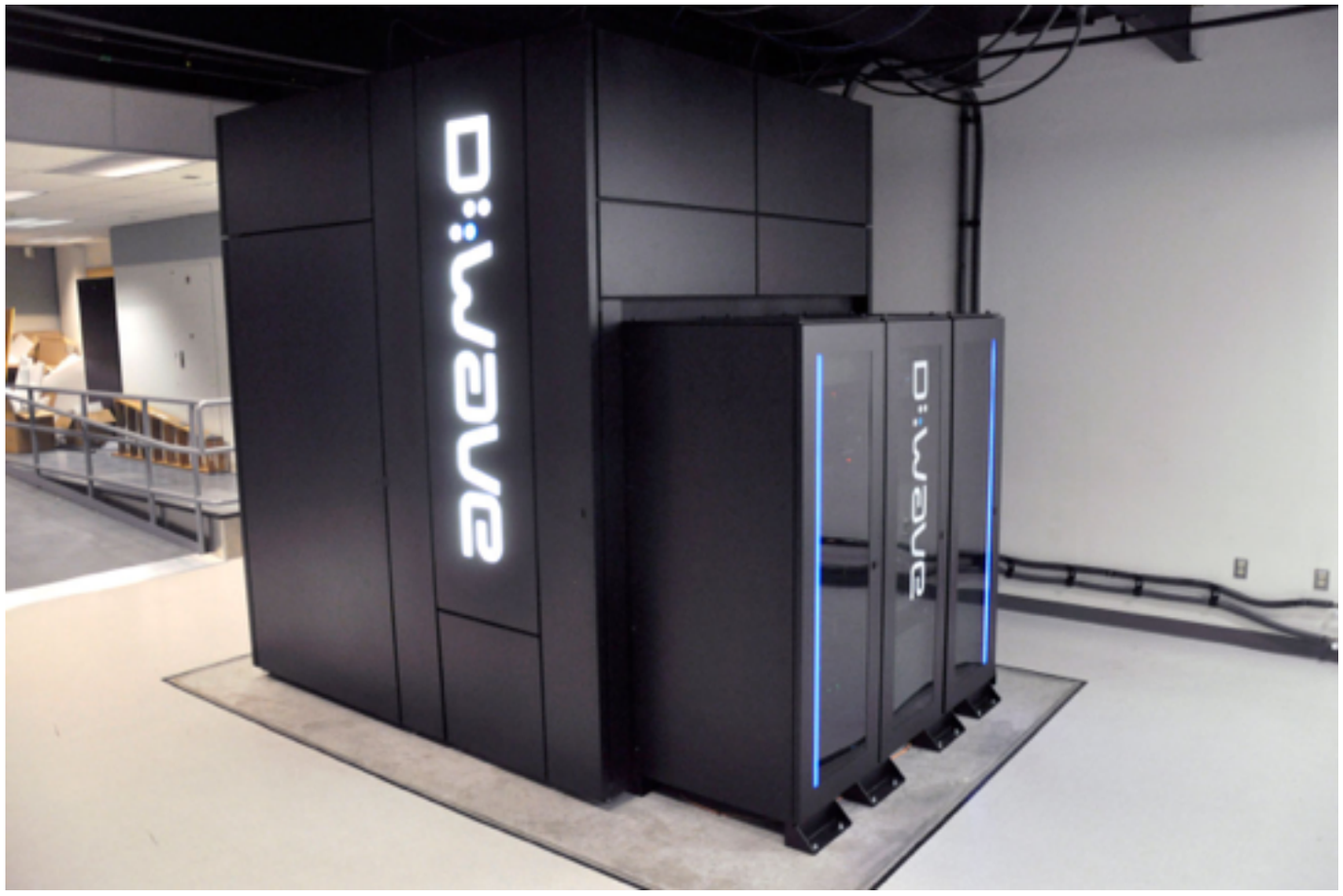
- Large signatures and keys too, stateful (evolving signing keys)

Ok for low-volume applications, like secure boot systems

Is D-Wave a threat to crypto?

The Quantum Computing Company™, since 1999

- Sold machines to Google, Lockheed, NASA
- Machines with ~1000 qubits in total



Is D-Wave a threat to crypto?

No

D-Wave machines just do **quantum annealing**, not the real thing

- Quantum version of simulated annealing
- Dedicated hardware for specific optimization problems
- **Can’t run Shor**, so can’t break crypto, boring

Not about scalable, fault-tolerant, universal quantum computers

Yet, they’re the best at what they do, but how useful is it?

Recent results/PR

Google says its quantum computer is 100 million times faster than PC

Controversial D-Wave system gets thumbs up

Follows a paper from **Google**, http://arxiv.org/abs/1512.02206

- Evidence that D-Wave's machine is fast on some problems
- Claims of a 10^8-fold speed-up in some cases
- Too good to be true?

Researchers debunked the speedup claim

- D-Wave is **not faster** than classical computers (just slow ones)
- Details on http://www.scottaaronson.com/blog/?p=2555

Conclusions

If you manage Top Secret-class information then, in this order:

1. Always encrypt it (in-transit, at-rest)
2. Protect the keys and passphrases (use secure hardware etc.)
3. Do your best to prevent leaks/blackmail/espionnage
4. Use at least RSA-3072 if RSA, 256-bit curves if ECC
5. Use at least 256-bit symmetric keys

You've done all this? Congrats, you're in the top 1%

Now you may worry about quantum computers and PQC