Quantum Computing and Cryptography on the Internet

Paul Hoffman

LAC Domain Name Week
26 April 2022

Overview of today

- This is a deep topic worthy of long academic papers
- 20 minutes of talk; 10 minutes of questions
- ICANN has a more detailed paper on this, but even that can only skim the surface of the topic
- The links at the end of these slides go into *much* more detail

The threat

- In the future, very large quantum computers may be able to determine the private keys used today in DNSSEC and TLS, as well as most other popular security protocols
- For DNSSEC, this means that someone with such a computer could impersonate any zone owner who signs with DNSSEC, even the root
- For TLS, this means that any private exchange that has been recorded could be exposed by such a computer
- These quantum computers are not ready now (or even soon), but might be available in future decades

Quantum computers

- Made up of quantum bits (qubits), which hold quantum state
- Qubits that are entangled with each other allow instantaneous parallel computation that is unavailable in silicon-based computers
- Qubits are extremely susceptible to environmental noise, and thus need to be kept at near-zero Kelvin during computation
- Real quantum computers need error correction of 100s or 1000s of qubits to make an “effective” qubit

Building large quantum computers

- Unless error correction can get much better, breaking today's cryptography will require quantum computers that have more than 10 million qubits
- No one knows how to make such large computers, given the problems with interconnections between the qubits and the need for incredible cooling
- Given the immense cost of building large quantum computers, it is not clear when building such computers will be worth doing

What can be done to prevent the problem

- Using bigger keys will only delay when cryptographically relevant quantum computers (CRQCs) might be useful by a few years or decades
- New post-quantum cryptographic (PQC) algorithms have been described that are not susceptible to quantum computers
- These algorithms have much larger keys, much larger signatures, or both
- There are still strong arguments in the cryptography world about which of these new algorithms are secure enough to replace today's algorithms
- There are different PQC algorithms for signing and key exchange

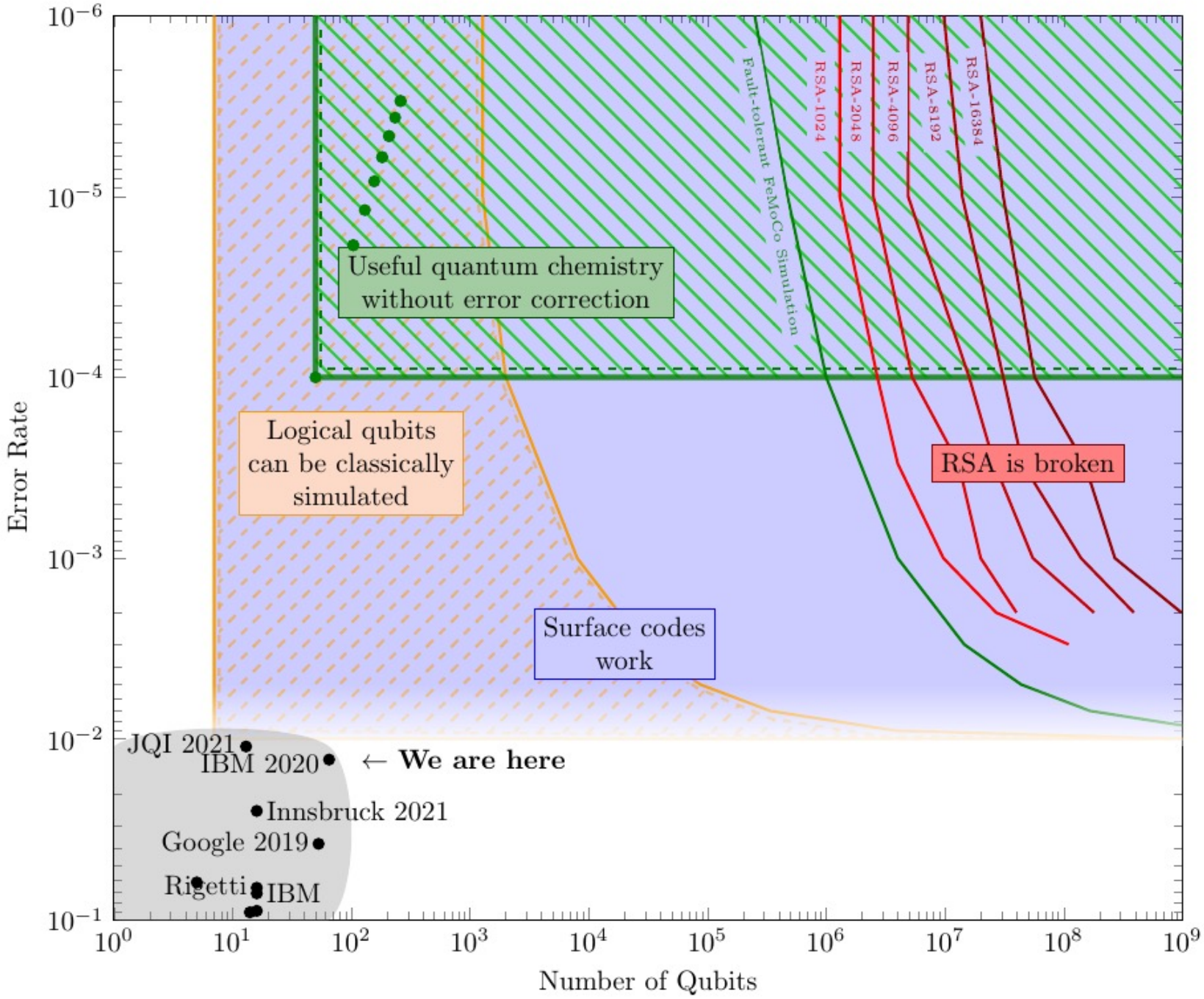
Ways forward

- For TLS, changing to PQC key exchange algorithms as soon as possible makes sense even if cryptographically relevant quantum computers (CRQCs) cannot be built in the next 20-40 years because some secrets need to be kept for many decades
- For DNSSEC, waiting until good PQC signing algorithms are stable makes sense because signing keys have shorter lifetimes, and DNSSEC currently has problems with large keys and signatures
- Other protocols that use public key cryptography also need to be updated
- Almost all the current focus is on developing PQC key exchange algorithms, so waiting for the focus to change will yield better algorithms for DNSSEC

Will quantum computers keep getting better? Yes!

- However, progress on making CRQCs is very slow due to difficult physics (making fast and stable qubits) and difficult engineering (cooling huge quantum circuits while still allowing useful computations)
- The real question is how fast will useful quantum computers get better, and this depends on their usefulness
- There are many potential problems quantum computers might solve better than today's computers, but the value of solving these problems may be lower than the cost of developing large quantum computers
- It all comes down to cost and economic motivation
- Protocols that need PQC key exchange algorithms will have them within a few years

Where we are today



Questions?

- ... and links!
  - Quantum Computing and the DNS, OCTO-031
  - Internet Security and Quantum Computing, by Hilarie Orman
  - Landscape of Quantum Computing in 2021, by Sam Jaques
  - Quantum Technology and Its Impact on Security in Mobile Networks, by Ericsson
  - Quantum Computation and Quantum Information, 10th Anniversary Edition, by Michael Nielsen and Isaac Chuang

Engage with ICANN

Thank You and Questions

Visit us at **icann.org**
Email: paul.hoffman@icann.org

@icann

linkedin/company/icann

facebook.com/icannorg

slideshare/icannpresentations

youtube.com/icannnews

soundcloud/icann

flickr.com/icann

instagram.com/icannorg