Quantum Computing and the DNS

Paul Hoffman
ICANN Office of the CTO

ICANN73 DNSSEC and Security Workshop
9 March 2022

Overview of today

- Quantum computers in the future can decrypt stored TLS sessions and find the public keys for DNSSEC
- ICANN has just published a more detailed paper on this, but even that can only skim the surface of the topic
- Lots of links a few slides from now

The threat to the DNS

- 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

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**

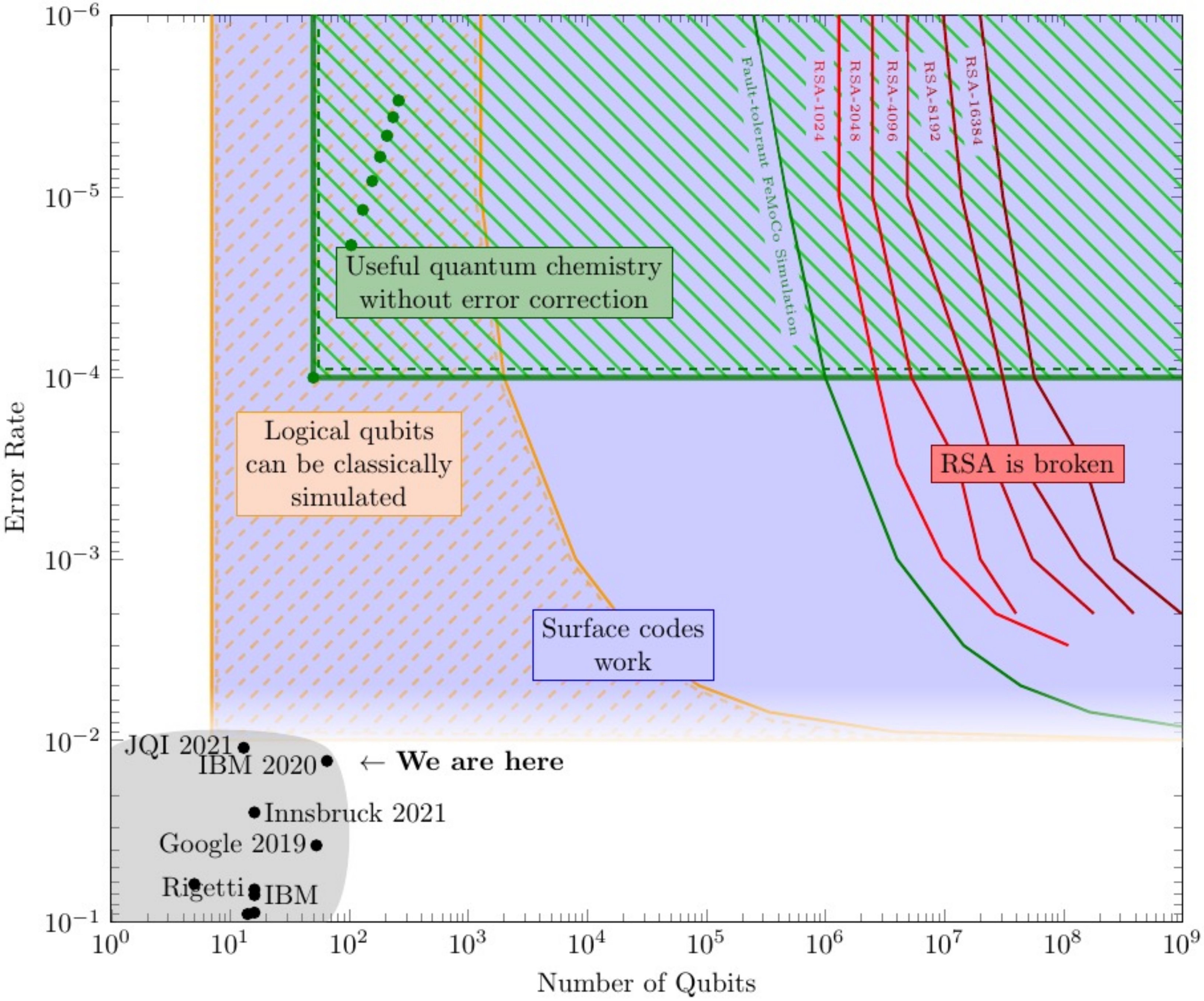
- **No one knows** today how to make such large computers, given the problems with interconnections between the qubits and the need for incredible cooling

- Given the immense cost of building large quantum computers, it is not clear **when** building such computers will be worth doing even with the attractive target of breaking today’s crypto

Recent relevant publications

- 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

Getting from here to there



What can be done to prevent the problem

- Using bigger DNSSEC and TLS keys **will only delay** when cryptographically relevant quantum computers (CRQCs) might be useful by a few years or decades
- Many new post-quantum cryptographic (PQC) algorithms have been described that are **not susceptible to quantum computers**
- There are different PQC algorithms for signing and key exchange, and they must be **analyzed separately**
- 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

Ways forward for the DNS community

- 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!

- 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 high cost of developing large quantum computers
- **It all comes down to cost and economic motivation**
- Attackers will probably get **more value** out of viewing previously-private TLS and IPsec traffic, and forging web PKI certificates, than forging DNSSEC signatures

Engage with ICANN

ICANN

Thank You and Questions

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

- @icann
- facebook.com/icannorg
- youtube.com/icannnews
- flickr.com/icann
- linkedin/company/icann
- slideshare/icannpresentations
- soundcloud/icann
- instagram.com/icannorg