Quantum Computing and the DNS

Champika Wijayatunga

VNNIC Internet Conference 2025
25 July 2025

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
- Cryptographically relevant quantum computers (CRQCs) are **not ready now** (or even soon), but might be available in future decades
- For DNSSEC, this means that someone with such a computer **might be able to** impersonate any zone owner who signs with DNSSEC, even the root
- For TLS, an attacker can be collecting traffic now to decrypt later with a CRQC

Quantum computers

- **Not at all** like any of today's common computers
- Made up of quantum bits (**qubits**), which hold quantum state
- Qubits are extremely susceptible to environmental noise, and thus need to be kept at **near-zero Kelvin** during computation
- To be **useful**, quantum computers must be better than classical computers, but we have no idea when those quantum computers can be built
- CRQCs are particularly large, and thus **harder to build**

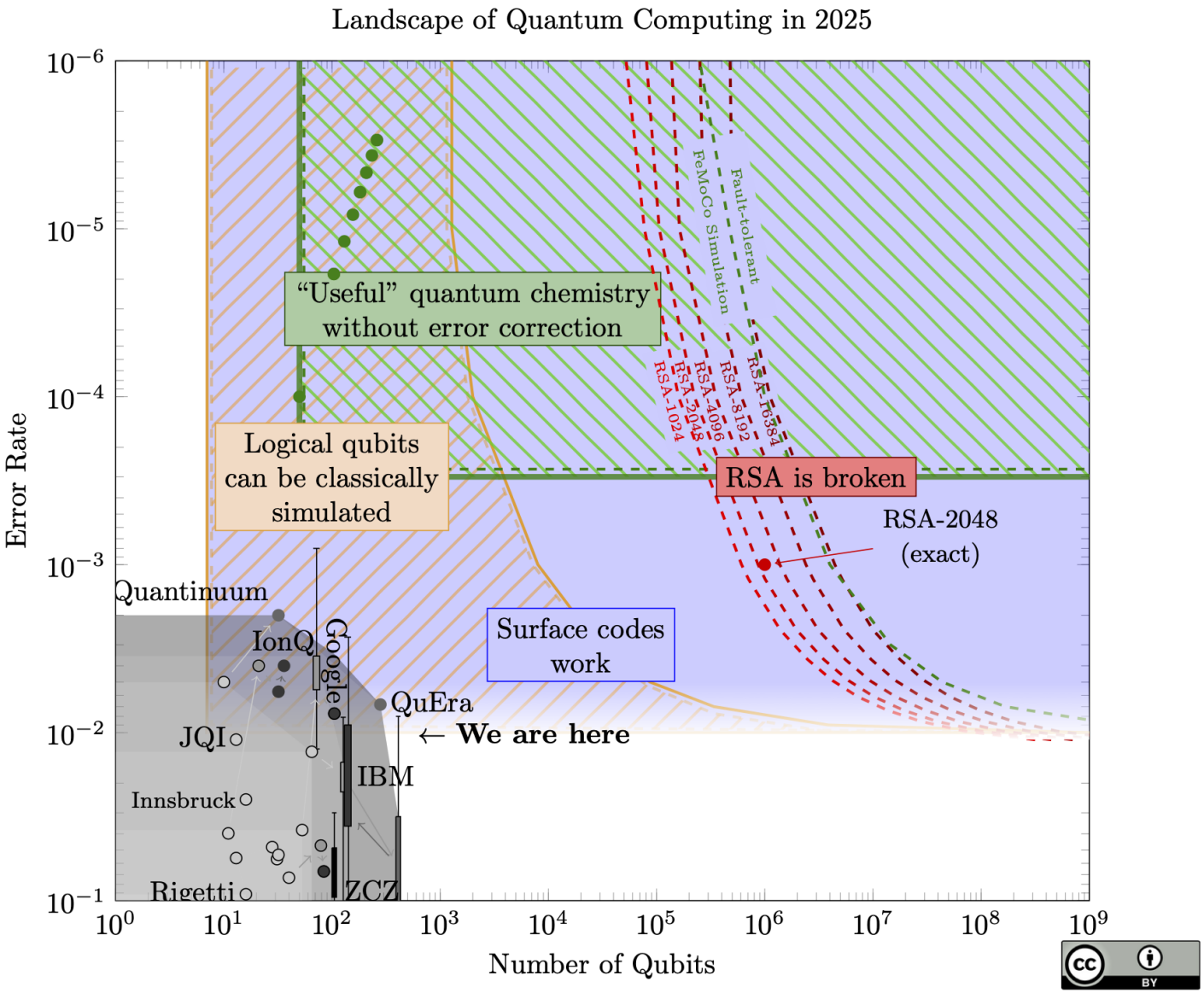
What can be done to prevent the cryptography problem

- Using bigger keys today **will only delay** when CRQCs might be useful by a few years or decades
- New post-quantum cryptographic (**PQC**) algorithms have been developed that are not susceptible to quantum computers
- These algorithms have **much larger keys, much larger signatures, or both**
- PQC algorithms are an active area of research and standardization, and some are already being deployed

Ways forward

- OCTO-031 gives ICANN's position on what to do
- For DNSSEC, waiting until **good PQC signing algorithms are standardized and stable** makes sense because signing keys have shorter lifetimes, and DNSSEC currently has problems with large keys and signatures
- OCTO-031 also covers TLS (used in DNS-over-TLS, for example); in short, **let's go quickly** on these
- Lots of work in the IETF and IRTF on analysis and standardization

Where we are today



Questions?