What DNS Admins Should **Know** About Post-Quantum Cryptography

Paul Hoffman, ICANN

DNS-OARC 26, May 2017

Madrid

v3

The problem, and the solution

- You get asked the question "**What are we doing** about post-quantum crypto?"
- Correct answer: "We're **following the discussions** about the new algorithms and about when in the future we will need to start using them"
- This presentation is what you should **know** about post-quantum crypto, not what you should **do** about it

Quantum computing in one slide

- **Qubits**: bits that return values between 0 and 1
- To be interesting, the qubits need to be connected by **quantum gates** into **quantum circuits** that represent a **quantum algorithm**
- Measurement destroys the value in the qubits in the circuit
- Useful for searching in some ways that classical computers cannot do efficiently
- There are approximately five different quantum technologies that might work at scale
- **Large-scale quantum computers** may be feasible to build in the future

Quantum computers and DNSSEC signatures

- **Signing algorithms** use cryptography whose strength is based on the difficulty of factoring (RSA) or determining discrete logs (elliptic curve)
- Large-scale quantum computers with **quantum Fourier transform circuitry** significantly reduce the difficulty of both of those problems
- Using **Shor's algorithm**, finding the private keys takes many fewer steps
- If large-scale quantum computers become feasible, **it is not clear** whether RSA or elliptic curve keys **will fall first**

Post-quantum cryptography

- **Post-quantum cryptography** is signature and key exchange algorithms that **cannot be weakened** by Shor's algorithm
  - Also symmetric algorithms, but that's ignored here
- They use different cryptographic primitives
- **However**, in order to be as strong as current algorithms, the keys and/or the signatures are much larger (**10s of thousands of bits** through millions of bits)
- NIST is taking submissions for a competition, but doesn't expect to pick a standard for **many years**

There are no cryptography-busting quantum computers yet

- Building large-scale quantum computers is **difficult and expensive**
- Qubits need a lot of **error correction**; maybe 1000-to-1 to fix current problems
- Some designs need milli-Kelvin temperatures
- To break **2048-bit** RSA curve keys, you need a circuit with at least 4099 qubits, and to perform **100 billion operations**
- So far, the ones maybe implementing Shor's algorithm have **less than 10 qubits**

Determining when quantum computing will affect DNSSEC

- **Proposal**: demonstration of breaking 512-bit RSA keys or 64-bit elliptic curve keys should alert the world for 2048-bit RSA or 256-bit elliptic curve
  - Again, ignoring symmetric algorithms here
- This will tell us which quantum technology is **likely to be feasible** and the likely roadblocks
- We will **certainly not hear** how well the NSA, the FSB, and others are doing with their internal developments, of course

What to do when current keys become vulnerable

- If RSA keys become vulnerable first, **switch** your DNSSEC keys to larger elliptic curve (maybe 512-bit keys)
- If elliptic curve keys become vulnerable first, **switch** your DNSSEC keys to larger RSA (maybe RSA-8192)
- See what NIST (or others) have **standardized** for post-quantum algorithms

What's next for DNSSEC admins

- Draft in **CFRG** about determining when large-scale quantum computers that affect cryptography might be feasible
- Watch if Shor's algorithm gets **practical uses** outside of breaking cryptography
- Make sure that we can **roll algorithms**