Quantum Cryptography Update

CA/Browser Forum

Thessaloniki, GR

2019-06-12

Overview

- Upcoming Events
- Blog Post
- Papers
- Next Steps

Upcoming Events

- Second PQC Standardization Process (NIST)
  - August 22-24, Santa Barbara

Since March…

DigiCert on Quantum 2: When Will Cryptographically Relevant Quantum Computers Arrive?

https://www.digicert.com/blog/digicert-on-quantum-2-when-will-cryptographically-relevant-quantum-computers-arrive/

When Will Cryptographically Relevant Quantum Computers Arrive?

- Three takeaways:
  - Don’t just count qubits
  - US NAS: Growth of quantum computers likely to be based on economic utility
  - ETSI QSC: Things may go quickly if traditional chip fab techniques can be leveraged (and slower if not)

Papers

- **How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits**

https://arxiv.org/abs/1905.09749

Next Steps

Cryptographic transitions are measured in decades …

Very preliminary work going on at IETF on how the transition will work

Email discussion list?

- Some additional people have expressed interest in joining the discussion …