Quantum Computers and Cryptography

By Johann Winter

Modern Cryptography

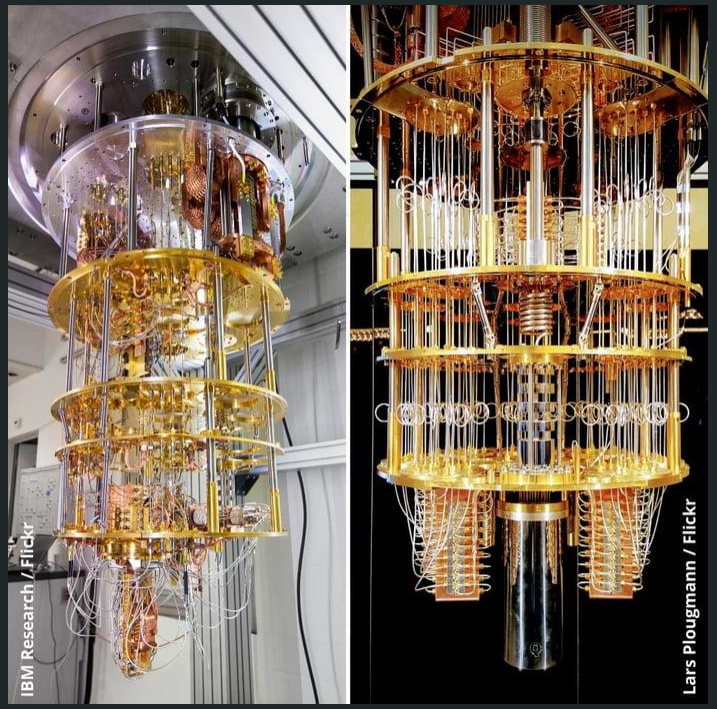
- Asymmetric Encryption
  - Prime Factorization
  - Elliptic Curve
- Symmetric Encryption
  - Substitution Box

- Secures everything in the digital world
  - Websites
  - Emails
  - Messaging apps

Quantum Computers

- Qubits
- Makes use of quantum properties of certain particles

- Quantum specific algorithms
  - Search Algorithms
  - Minimization Problems
  - Neural networks

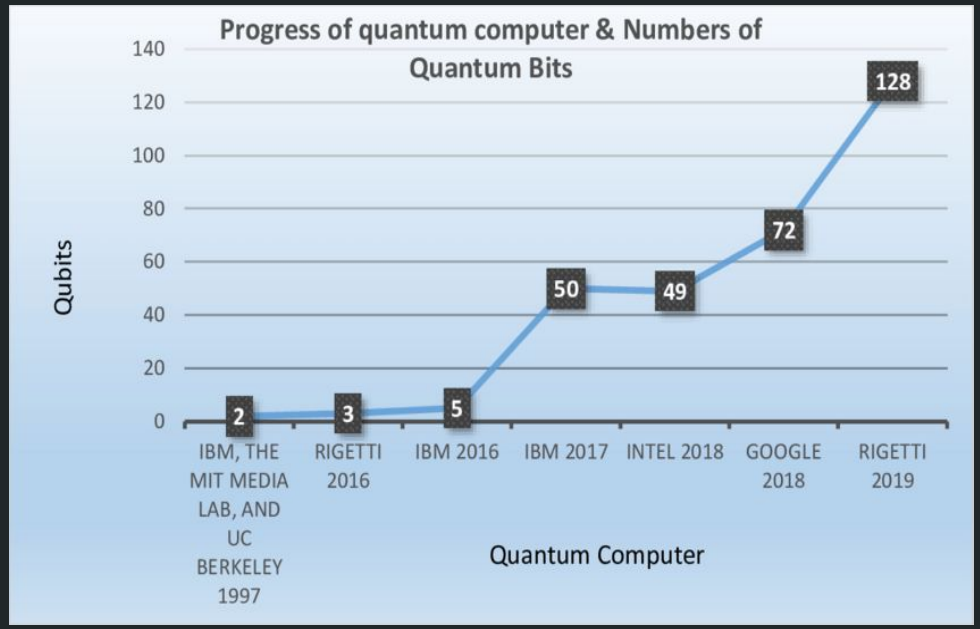


IBM’s 53-qubit quantum computer

Quantum Threat to Cryptography

- Shor’s Algorithm
  - Asymmetric Encryption

- RSA 2048 requires a few million qubits to be cracked in eight hours



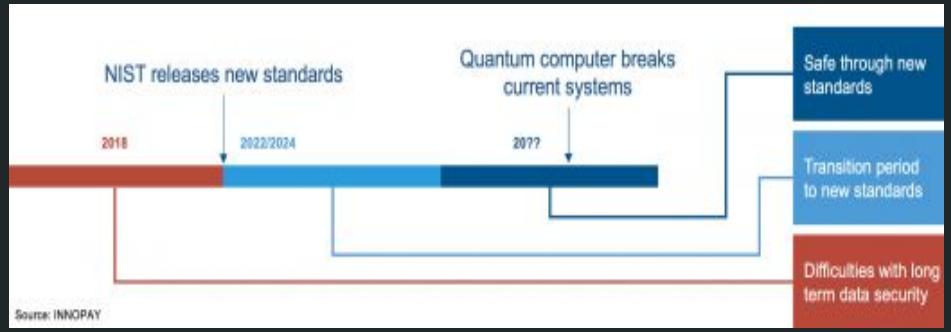
Why is this an issue?

- Encrypted data is safe now, but not in the future

- Saving encrypted data
- Crack encryption when sufficiently powerful quantum computers are available

Post-Quantum Cryptography

- NIST - National Institute of Standards and Technology
- Project began in 2016
- PQC Algorithms are planned to become standardized by 2024
- 15 PQC algorithms remain in round 3
- Certain implementations already exist
  - OpenSSL
  - OpenSSH



Conclusion

Use post-quantum cryptographic algorithms as soon as possible

Be mindful of encryption and trust

Citations

Computer Security Division, Information Technology Laboratory. “Post-Quantum Cryptography: CSRC.” CSRC, https://csrc.nist.gov/projects/post-quantum-cryptography.

arXiv, Emerging Technology from the. “How a Quantum Computer Could Break 2048-Bit RSA Encryption in 8 Hours.” MIT Technology Review, MIT Technology Review, 2 Apr. 2020, https://www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/.