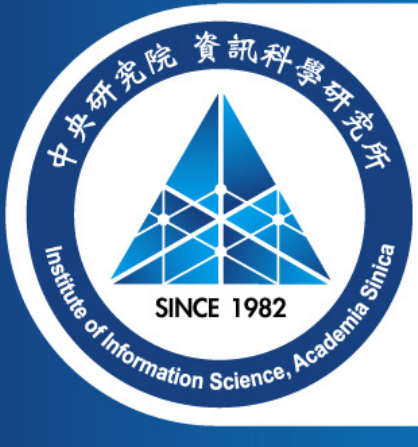


量子電腦對密碼學或資安的影響:

Impact of Quantum Computing on Cryptography and Cybersecurity

楊柏因 Bo-Yin Yang

2024 年 5 月 16 日, @ 資安大會

What Quantum Computing Is and Isn't

Contrary to common misconceptions, a Quantum Computer is simply *different*

What a Quantum Computer is *not*

Not Faster: "Quantum gate" 4-6 orders of magnitude slower than a regular gate.

Not Traditionally Structured: No entanglements-at-a-distance.

Not a Computer: It is fundamentally different, capable of different things.

What Can a Quantum Computer Do?

Shor's Algorithm: *hidden subgroup problem*

Grover's Algorithm: *search problem*

Kuperberg's Algorithm: subexponential speed-up on a *hidden shift problem*

At the moment, almost nothing that doesn't break cryptosystems!

Pessimistic About the Advances of Quantum Computing, Why?

Super-Moore Advances Projected, I say not by a long shot

- No killer applications, no financial gain
- Fundamental technical problems still need to be solved.
- Omnipresence impossible (maybe except for neutral trapped atom qubits)

This (superexpert) opinion likely over-optimistic

⇒ Michele Mosca, University of Waterloo:
"1/7 chance of breaking RSA-2048 by 2026, 1/2 chance by 2031".

⇒ Yet **who knows?** So, need to prepare, because risk management.

We still expect 10–15 years

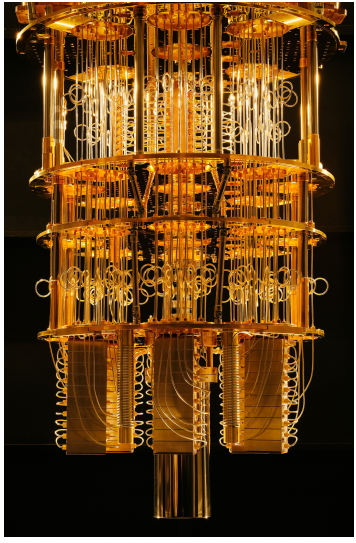
- because Nation-State Actors
- and someone might come up with something for a Nobel Prize

What would Quantum Computing do to IT Security

Problem:

- **Grover's algorithm** gives a quadratic speedup on search problems:
  - *symmetric cryptography* is in danger (in particular **AES-128**).

  ⇒ Double the key length!



What would Quantum Computing do to IT Security

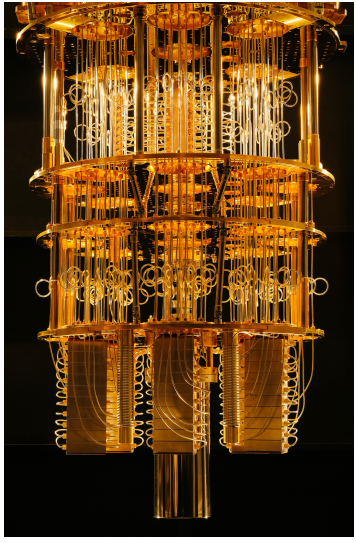
Problem:

- **Grover's algorithm** gives a quadratic speedup on search problems:
  - *symmetric cryptography* is in danger (in particular **AES-128**).

  ⇒ Double the key length!

- **Shor's algorithm** solves the "hidden-subgroup problem" in finite abelian groups:
  - *asymmetric cryptography* is broken (**RSA, DH, DSA, ECDSA, ECDH, ...**)!

  ⇒ New schemes are required!

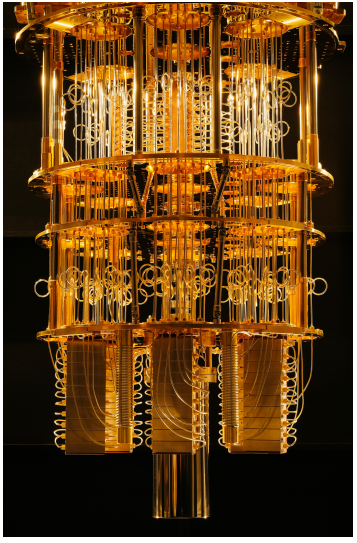


Threat Level:

- Store Now, Decrypt Later

  ⇒ Michele Mosca, University of Waterloo:

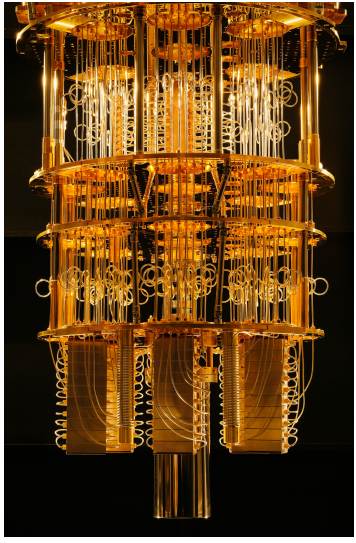
  "If your secret needs to be kept for X years, postquantum transitions Y years, and only Z years until a CRQC, then you are in trouble if X + Y > Z."



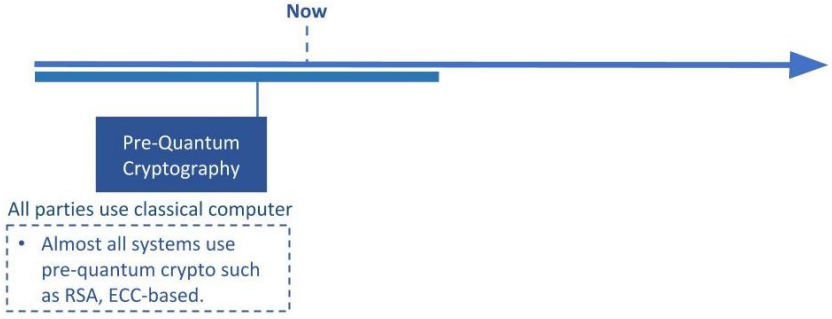
Quantum Computing and IT Security

Threat Level:

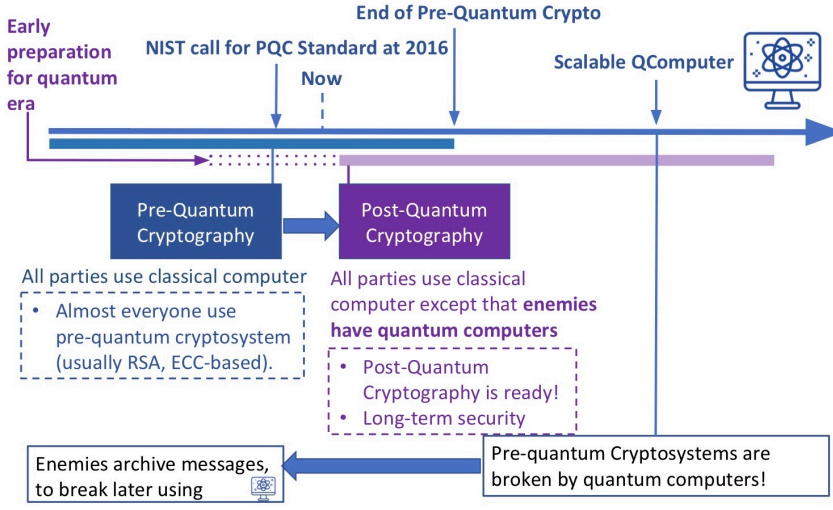
- Store Now, Decrypt Later
  - ⇒ Michele Mosca, University of Waterloo:
    "If your secret needs to be kept for X years, postquantum transitions Y years, and only Z years until a CRQC, then you are in trouble if X + Y > Z."
- Already today systems and products are affected that have a long life-span or that handle sensitive data:
  - chip manufacturing, critical infrastructure, medicine, business and state secrets...



Quantum Computing and IT Security

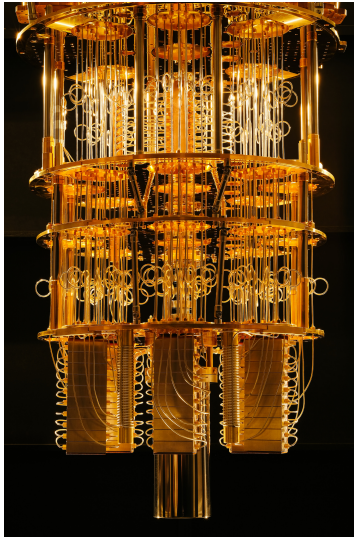


Quantum Computing and IT Security



Solution 1:

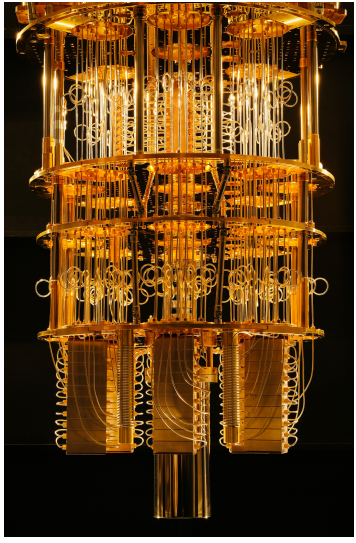
- **Quantum Cryptography** (Ambiguous term usually = *Quantum Key Distribution*)
  - Expensive, hard to secure
  - Limited functionality (only confidentiality)
  - Needs pre-shared keys or post-quantum digital signatures for authentication.
  - last-mile problem to your iPhone?
- Still need algorithmic crypto to be secure



Solution 2:

- **Post-Quantum Cryptography:** Ready Today!
  - Design, implementation, evaluation, and integration of alternative schemes:

  ⇒ hash-based,
  ⇒ code-based,
  ⇒ lattice-based, and
  ⇒ multivariate schemes.
  ⇒ isogeny-based schemes.
- To-be standards: Kyber(ML-KEM), Dililithium(ML-DSA), SPHINCS+(SLH-DSA), Falcon (FN-DSA)
- In the Running: Classic McEliece, HQC, BIKE



Post-Quantum Cryptography

- 1994 Shor's algorithm.
- 2003 "Post-Quantum Cryptography (PQC)" coined.
- 2006: First International Workshop on Post-Quantum Cryptography (15 since)
- 2014: EU solicits proposals in post-quantum crypto
- 2014: ETSI starts "Quantum-safe" crypto workgroup.
- 2015.04: NIST PQC workshop, NSA PQC announcements
- 2016 NSA announcement, NIST calls for submissions of public-key cryptosystems to "Post-Quantum Cryptography Standardization Project". After public input.

Post-Quantum Cryptography

- NIST standardization process (2016–):
  - about 82 submissions,
  - schemes from all PQC families,
  - *signature algorithms* and
  - *key encapsulation*.
- Some Tough Cuts
  - 69 Round-1 Schemes 2017.12.21
    - One broken that night!
  - 26 Round-2 schemes 2019.01.31
  - 15 Round-3 schemes 2020.07.23
  - 4 Standards, 4 Round-4 schemes announced 2022.07.05
- Supplementary Round for Signatures (40 submissions) now

Thanks for Listening!

I'll field any questions, but talks from Dr. Kannwischer and Professor Lange should answer most if not all.