NIST Crypto Short Talk: Quantum Computing

August 13, 2021

Carl A. Miller

Disclaimer: This is **not** a scientific talk.

(I’m just interpreting what other sources have said about quantum computing.)

Context

M. Mosca

Is x + y < z?

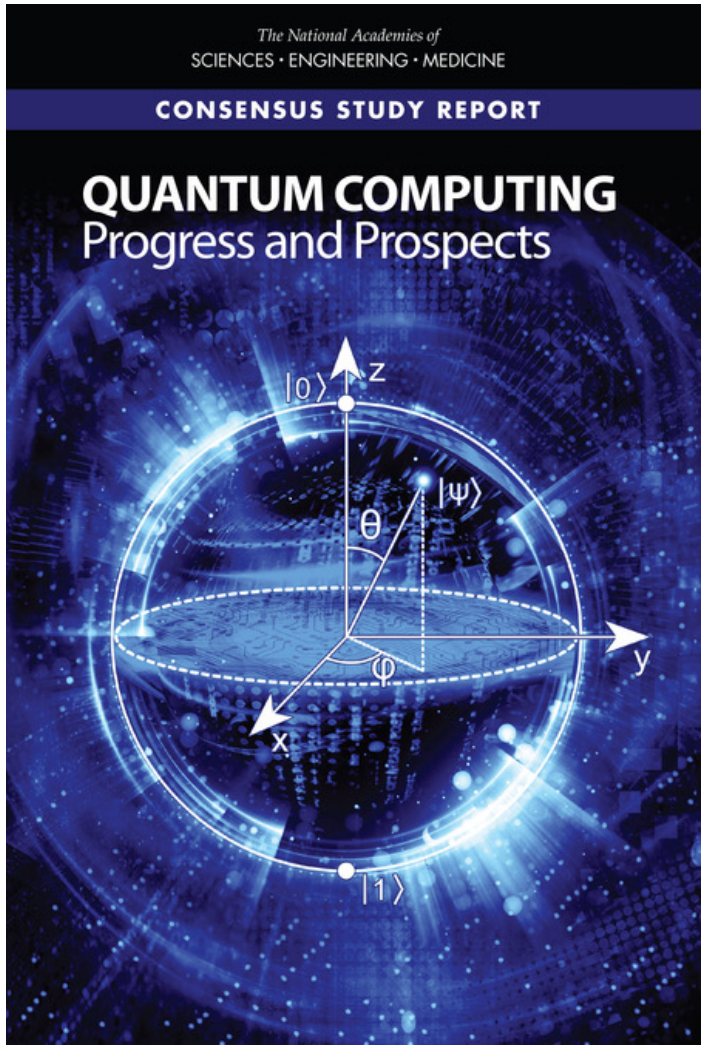
x = time frame to implement postquantum crypto

y = how long we want our cryptography to be secure

z = how long before quantum computers break old crypto

Sources

Trustworthy source. Pretty cautious & conservative in what it says.



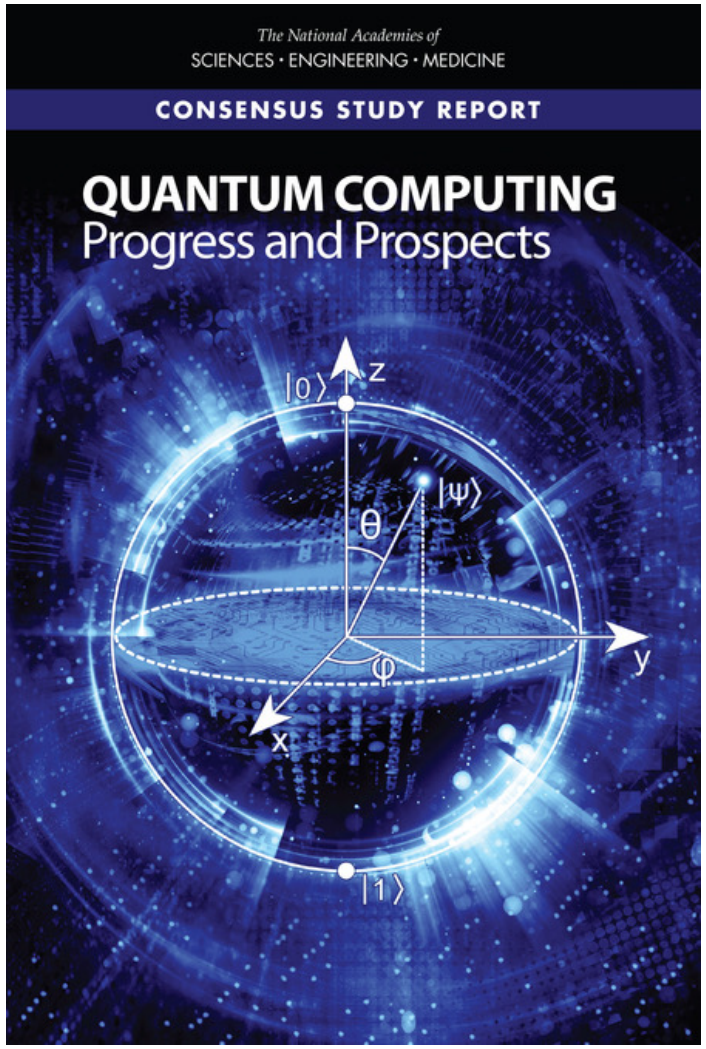
Sources

Takeaways:

- There's a ton of resources available to invest in quantum computing now.

- However, even those are not enough to implement Shor's algorithm.

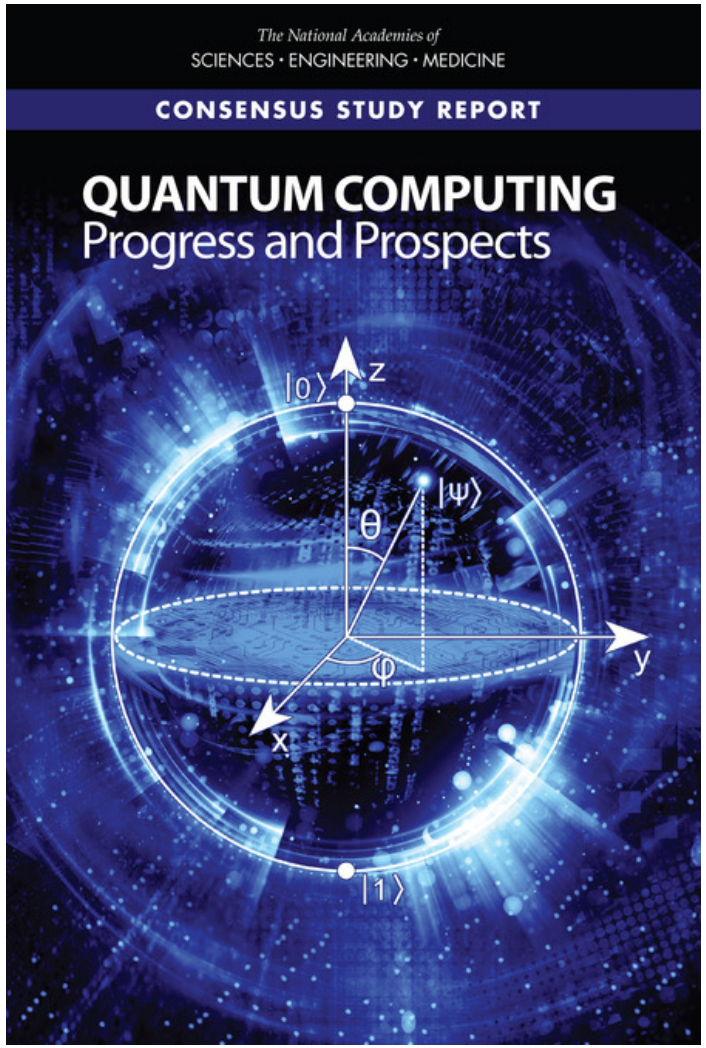
- A full-scale quantum computer will be built only if companies can profit from building intermediate-scale quantum computers first.



Sources

Takeaways:

- They agree that development of postquantum crypto is an urgent need.



Sources

Detailed & forward-looking, although obviously biased.

Google claimed to have achieved quantum supremacy in 2019.
This talk is about future work.

Talk: "Google's perspective on the viable applications of early fault-tolerant Quantum computers" (Ryan Babbush, July 30, 2021)

https://www.youtube.com/watch?v=-fcQt5C2XGY

Sources

Takeaways:

- Quantum algorithms providing a mere quadratic speedup are actually not much of a threat.

- Google plans to build a 1-million qubit fault-tolerant QC by 2029.

- Implementing Shor's algorithm would take 20 million qubits.

Talk: "Google's perspective on the viable applications of early fault-tolerant Quantum computers" (Ryan Babbush, July 30, 2021)

https://www.youtube.com/watch?v=-fcQt5C2XGY

Why is it difficult to predict the future of QC?

It's going to depend on choices made in the future.

Predictions may influence the outcome.

I don't know how seriously to take assertions like these →

Next 15 years:
Slightly more than half (23/44) of the respondents indicated "about 50%" likely or more likely, among whom 5 indicated a ">70%" likelihood, and 7 an even higher ">95%" likelihood. Still, half of the respondents (21/44) indicated "<30%" or even less likely.

"Quantum Threat Timeline Report 2020,"
M. Mosca, M. Piani

Are there any fundamental obstructions to QC?

What motivates near-term investments in QC?