Quantum's Impact on Security

Key Takeaways

MIT CSAIL

MIT Center for Quantum Engineering

INTRODUCTION
WITH CSAIL DIRECTOR PROFESSOR DANIELA RUS

Why it's important to be talking about quantum computing:

- The immense volume of data being created means we need a new way to process it.
  - 3.5 quintillion bytes of data were created every day in 2023.
  - Over 41 million messages are exchanged every minute by WhatsApp Users.
  - Every day we generate 250K libraries of congress, or the content of 5 million laptops.
  - With the number of global internet users growing all the time, this problem will only get worse.
- Quantum computing is a threat to modern-day security systems.
  - The strength of current cryptographic systems traditionally hinges on the computational impracticality of breaking them.
  - Quantum computing is set to disrupt this previously impenetrable system.
  - However, quantum itself might also provide the opportunity for a solution with ideas like the no cloning theorem, quantum entanglement, and more.

"Quantum computing represents more than just rapid computational speeds and unparalleled processing powers.

Quantum computing embodies a fundamental shift in our understanding and approach to computation."

MIT CSAIL

MIT Center for QuantumEngineering

www.cap.csail.mit.edu

WHERE QUANTUM COMPUTERS STAND

WITH DIRECTOR OF THE CENTER FOR QUANTUM ENGINEERING PROFESSOR WILLIAM OLIVER

- In comparison to classical computers, which have undergone over 100 years of development, quantum computers are relatively new.
- Recent ideas in error correction have “kick-started the field” by giving engineers a way to make quantum computers robust and applicable.
- We’ve gone from Quantum 1.0, which allowed scientists to use quantum physics to better understand how classical computers work, to Quantum 2.0, which means actually using quantum concepts to operate.
- There are currently several small-scale quantum computers in operation (IBM’s Eagle Processor,Google’s Sycamore Processor, etc.), and error correction schemes are now starting to be demonstrated with them.
- Error correction enables system **resilience through hardware redundancy**, although this redundancy necessitates larger, more expensive quantum computers.
- **The Takeaway:** Quantum computing is roughly in the stage that commercial flight was when the Wright Brothers first flew at Kitty Hawk. It will take collaboration, education, and money, but businesses should be preparing for a post-quantum world now, particularly when it comes to cybersecurity.

“Advancing from discovery to useful machines takes time, science, and engineering.”

MIT CSAIL

MIT Center for QuantumEngineering

www.cap.csail.mit.edu

WHAT ARE QUANTUM COMPUTERS GOOD FOR?

WITH PROFESSOR PETER SHOR

- The amazing classical computers we have today were made possible because computers were useful right at the beginning, meaning companies could sell them and use that money to “bootstrap” the technology.
- Small, early-stage quantum computers aren’t as obviously useful due to a lack of reliable error correction.
  - For example: to be useful in factoring, a quantum computer would need at least 2K logical qubits, which in reality means 1 million physical qubits.
- Some potential applications for quantum computers are:
  - Simulating physics problems (might not be lucrative enough)
  - Chemistry and drug design (require larger computers)
  - Quantum search through Grover’s algorithm (require larger computers)
  - Optimization (still speculative)
  - Quantum machine learning (still speculative)
- **The Takeaway:** experimentation is needed to find an application for early-stage quantum computers that will give the technology the funds and attention it needs to grow.

“I think there’s a lot of hope that we will get small quantum algorithms that will let people sell quantum computers, and then we will get this bootstrapping to get larger quantum computers.”

MIT CSAIL

MIT Center for QuantumEngineering

www.cap.csail.mit.edu

QUANTUM AND CRYPTOGRAPHY

WITH HEAD OF THE THEORY GROUP AT CSAIL PROFESSOR VINOD VAIKUNTANATHAN

- Rapid improvements happening in quantum computing right now means that we need to prepare for the eventual arrival of quantum computers. For the purposes of cryptography, this involves inventing new methods for public-key encryption and digital signatures.
- The most promising public-key cryptosystem out there uses lattice-based cryptography which uses the geometry of integer lattices to hide information.
- On the other hand, quantum information itself might also enable new capabilities, for example using the “no cloning theorem,” which tells us that quantum information cannot be copied.
  - Quantum money, for example, would be physically impossible to counterfeit and shows an example of how quantum can be a constructive force in cryptography, and not just a security threat.
- Cautionary notes: **“Cryptographers seldom sleep well.”**
  - It would be prudent to develop multiple options for post-quantum cryptosystems in case one of them fails. For this reason, Professor Vaikuntanathan recommends hybrid encryption systems which, while more expensive, would protect us if either the existing or the new encryption system is secure.
  - The future of cybersecurity will need investment in research. We also need to be educating a larger set of people who understand post-quantum systems and can therefore help invent, test, and deploy them.

“Nearly all the public cryptography that we're using on an everyday basis relies on the hardness of factoring very large numbers or solving the discrete logarithm problem. Both of these can be solved quickly in polynomial time if you have large-scale quantum computers”

MIT CSAIL

MIT Center for QuantumEngineering

www.cap.csail.mit.edu

PANEL DISCUSSION

SUMMARY

- The qubits of today are quite faulty, so while scaling is important, it's much more important to improve the quality of the qubits.
- Quantum computers are not a threat to RSA security yet, but Professor Oliver asks: "How long do you want your information to stay secure?" Malicious actors can save information now that they'll be able to decrypt when strong enough quantum computers are available.
- In order to protect information, we need completely new methods in cryptography. The best current idea is lattice-based cryptography, but developing alternative options such as hybrid systems, quantum-based options, etc. is important because, as Professor Vaikuntanathan says, "**Lattice based cryptography is the only game in town. That makes me worried. We should at least have a couple of them lying around**."
- Both quantum computers and the security systems needed to protect against them will require massive investment, time, and skilled workers. Since this transition will require such an enormous overhaul of both hardware and software, Professor Oliver says, "**It's not too late to start right now**."
- Government also has a role to play, through both policy and enabling international cooperation to ensure consistent progress.
- Ultimately, there are many unknowns in this field which means it's important to be considering it from every angle, preparing for what's to come, and staying up to date with the research coming out of places like MIT CSAIL.

KEY QUOTES

"The quantum computers we have right now are like toys, in that they don't have enough qubits to do anything and their qubits are incredibly noisy."
~ Professor Shor

"Make security-critical software more agile, more modular, and easier to swap out one crypto system for another."
~ Professor Vaikuntanathan

"Collaboration is critical at this early stage."
~ Professor Oliver

MIT CSAIL

MIT Center for Quantum Engineering

www.cap.csail.mit.edu

LEARN MORE & GET CONNECTED

www.cap.csail.mit.edu

Lori Glover
Managing Director,
Global Strategic Alliances
lglover@mit.edu

Glenn Wong
Associate Director,
Business Development and Client Relations
glennw@mit.edu

MIT CSAIL

MIT Center for QuantumEngineering