QUANTUM & AI: IMPACT ON SECURITY

OCTOBER 9TH, 2024

KEY TAKEAWAYS

MIT CSAIL

MIT Center for QuantumEngineering

WELCOME & INTRODUCTION

Professor Daniela Rus, Director of CSAIL; Professor William Oliver, Director of the CQE

"When we couple the decision-making power of AI with the speed and potential of quantum technologies, we really have the potential to transform so much." ~ Professor Rus





- As scientists continue to push the boundaries of AI, we are reaching computational limits that quantum computing could help us overcome.
- Quantum technology holds the promise to sense, communicate, and process information in ways that are unobtainable by conventional or classical means.
- Quantum technology can be broken into three main areas:
  - Quantum sensing, which works to improve sensitivity, drift, & spatial resolution.
  - Quantum communication, which strives to enable distributed quantum states.
  - Quantum computing, which aims to solve select problems that are intractable with classical computing.
- Quantum computing & AI stand to impact information security because of Shor's algorithm, which offers a pathway for how a theoretical quantum computer could break RSA encryption. This looming threat fuels a need for post-quantum cryptographic security measures and also a reason for companies to stay informed on the timeline and development of quantum systems.

PANEL 1: THE LATEST ADVANCES IN QUANTUM

Professor Ike Chuang, EECS & Physics
Professor Aram Harrow, Physics
Dr. Bharath Kannan, CEO, Atlantic Quantum

Dr. Miguel Paredes, Sr. Principal Research Scientist, Dell
Moderator: Professor William Oliver, Director of CQE

- The quantum computers of today are not yet economically useful, as they are too noisy and prone to error to provide meaningful results. Therefore, it is critically important in the near term to address error correction while simultaneously building hardware infrastructure that makes such machines feasible to use and apply to complex problems where there might be quantum advantage.
- Quantum computers will likely need to function in tandem with classical computers, leveraging classical elements (such as AI) for the larger scale parts of problems (like data storage and processing) and quantum for the smaller but complex parts (such as modeling quantum particles or protein interactions).
- Similarly, future data centers will likely combine elements of quantum and classical computing.
- The panelists were wary of the hype around quantum computing, emphasizing the dramatic improvements we've seen in classical computing (as a market competitor to quantum) and the long timeline before quantum computers will be able to prove their utility.
- However, just as classical computing technology evolved from vacuum tubes to transistors to integrated circuits, we can anticipate a similar evolution for quantum technologies leading to improved performance over time.
- There are also perhaps opportunities to creatively apply AI concepts toward quantum, such as the ability of diffusion models to create structured data out of random noise (such methods could potentially make use of the noisiness of quantum systems, although this is only speculative).
- AI has potential to help in quantum chip design, error mitigation, orchestration, and communication between the quantum and classical elements of the computer system. Whether quantum stands to improve AI is an open question.
- Since so much of the research in quantum algorithms and hardware is theoretical, the panelists agreed that the true potential of quantum computing won't be fully understood until there are functional machines being applied to real-world problems.

PANEL 1: THE LATEST ADVANCES IN QUANTUM

"The companies that are going to take advantage of quantum and really move the needle are the ones who are in it for the long haul, where the long haul is counted in decades."

~ Professor Oliver



PANEL 2: QUANTUM, AI, & SECURITY

Professor Vinod Vaikuntanathan, EECS
Assistant Professor Anand Natarajan, EECS
Juliette Peyronnet, US General Manager, Alice & Bob
Moderator: Professor Daniela Rus, Director of CSAIL

- In the realm of theory, the last year has seen major advances in optimizing Shor's algorithm, meaning that the arrival of a system which can break RSA security seems to be drawing closer.
- The current leading candidate to replace RSA encryption is lattice based cryptography, which resists quantum algorithms to the best of our knowledge. However, Professor Vaikuntanathan emphasized the need for extensive robust testing before it can be considered fully safe from quantum systems.
- It's important for businesses with sensitive data to be aware that, even though RSA-breaking quantum computers are not yet here, their data is still vulnerable. It is possible for malicious actors to gather and store encrypted data now for decryption at a later point when quantum computers become available.
- Professor Vaikuntanathan recommends those with information security concerns implement what he calls "onion encryption," or encrypt the data first with RSA and then use lattice based encryption on top of that for maximum security.
- AI might be useful to discover new ways of attacking these systems or generate ideas for new encryption schemes, but the future of these methods will depend on the ability of developers to see inside these AI systems and prove/verify that a scheme is actually secure.
- As with the other panel, there was general agreement that our understanding of how quantum will impact cybersecurity will improve dramatically when there are quantum machines available, and such improvement will likely bring with it new and creative solutions to cybersecurity problems.

PANEL 2: QUANTUM, AI, & SECURITY



“Large players need to take the lead in deploying these security systems.”
~ Professor Vaikuntanathan



“Cybersecurity is like flossing: everyone knows that you have to do it but hardly anybody does it.”
~ Professor Rus

STARTUP SHOWCASE

Qunett

Qunett is developing scalable hardware solutions for quantum device connectivity that integrate with existing infrastructure to enable deployable quantum networks. At the event, Qunett presented a demo of their quantum memory system.

QuEra

QuEra operates the world's largest publicly accessible quantum computer based on neutral atoms, which is widely recognized as a promising quantum modality. Users can access their quantum computer today on the cloud. Expanding on this technology, they are working to develop large-scale quantum computers to tackle classically intractable problems.

AltaStata

AltaStata protects data in multi-cloud environments and AI/ML ecosystems from malicious users and accidental misconfigurations without compromising utility or speed. They offer data encryption, compression, accessibility, and protection against data poisoning with AI.

Alice & Bob

Alice & Bob pioneered the Cat Qubit, the first qubit with built-in error correction. Using this technology, Alice & Bob aims to pave the way for fault-tolerant and universal gate-based quantum computing. Learn more about Alice & Bob in their CSAIL Alliances Case Study.

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 Quantum Engineering