CyLab Carnegie Mellon University Security and Privacy Institute

Carnegie Mellon University Software Engineering Institute

Organizational Readiness for Quantum Computing

OCTOBER 04, 2023

DR. THOMAS P. SCANLON
Technical Manager & Senior Research Scientist

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM23-1058

Quantum Computing

Classical Computing (Today's Common Computer)

Built on binary logic of bits (0 or 1) represented by binary physical property

Quantum Computing

Built on quantum bits (qubits) which can be in a superposition of two states at the same time

Represent both 0 and 1 at the same time

Superposition Coin Toss Analogy

Classical computer represents coin as ***only*** heads or tails after coin lands

Quantum computer can represent coin as ***both*** heads and tails at the same time while it is flipping in the air

Entanglement

Allows separated qubits to interact simultaneously

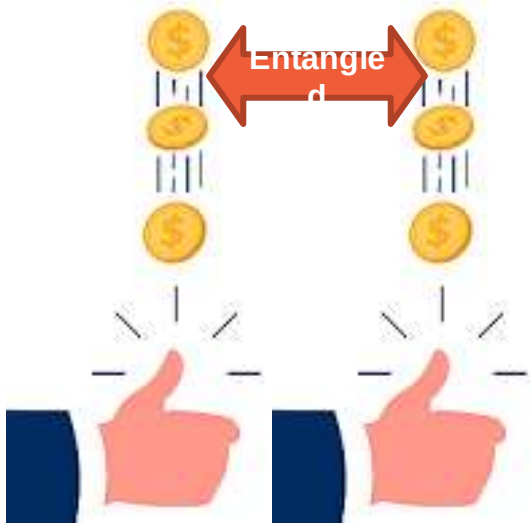
- Even when separated by significant distances
- Enables distributed encoding of data

Occurs when each particle's quantum state interact and cannot be described independently from state of other particles

- This means measured states of entangled particles are correlated such that measurement of state for a single particle enables probabilistic prediction of state for other particles

Revisiting the Coin Toss Analogy

- There are now two coins flipped at the same time
- As they are flipping, states of each coin are correlated



The Quantum Advantage

The Power of Quantum Computing

Superposition and Entanglement, in combination, enable substantial computing power

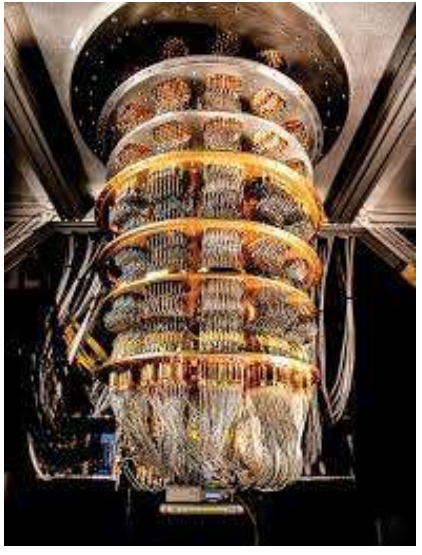
- **Classical 2-bit register:**

  Can store ***only one*** of four binary combinations (00, 01, 10, 11)

- **Quantum 2-qubit register:**

  Can store ***all four*** simultaneously

As more qubits are added, this computational advantage grows exponentially!



What Can Organizations Do Now?

Prepare for Post-Quantum Cryptography

- **Inventory critical datasets that must be secured for an extended amount of time.**
- **Inventory of all the systems using cryptographic technologies.**
- **Identify where and for what purpose public key cryptography is being used and mark those systems as quantum vulnerable.**
- **Prioritize date sets and system for cryptographic transition**
- **Using the inventory and prioritization information, organizations should develop a plan for systems transitions upon publication of new post-quantum cryptographic standards.**

For more detail: https://www.dhs.gov/quantum

What Can Organizations Do Now?

Beyond Post-Quantum Cryptography

- **Increase engagement with standards developing organizations in order to stay current with latest developments.**
- **Cybersecurity officials within organizations should identify acquisition, cybersecurity, and data security standards that will require updating to reflect post-quantum requirements.**
- **Develop quantum use-cases**

How can your organization take advantage of quantum computing power?

Potential Applications of Quantum Computing

Optimization

- Parallelization of computation to handle large numbers of operation simultaneously

Artificial Intelligence and Quantum Machine Learning

- Utilizing quantum parallelism to make better predictions and decisions by combinatoric processing of very large quantities of data

Chemical and Biological Engineering

- Discovery and manipulation of molecules and subatomic particles to help model and predict new molecule configurations
- Acceleration of materials discovery and drug development

And many others…

- Financial market modeling and predictions
- Complex manufacturing process failure detection
- …many intractable problems may become tractable

Contacts

Thomas Scanlon
Technical Manager
Senior Research Scientist

Telephone: +1 412-268-5800
Email: info@sei.cmu.edu