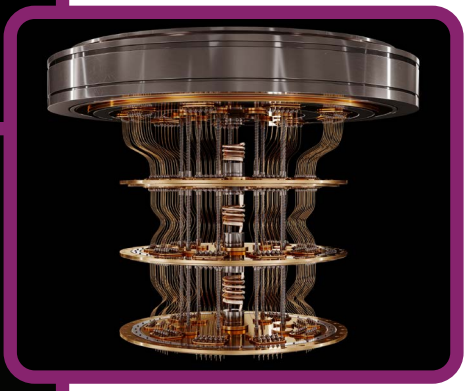
Quantum Cybersecurity Superposition

Division of Information Security
MAY 2023

Quantum Computing



Computing is on the edge of taking a leap based on quantum mechanics. Existing computing stores data in bits, in which all data is measured in values of one and zero. Quantum computing is based on quantum mechanics and its superposition theory that, at a sub-atomic level, particles can simultaneously exist in two opposing states. Using quantum bits, called q-bits, for data storage allows quantum computers to process data exponentially faster and in a fundamentally different manner than existing computers do.

The Leap Forward

Quantum computing holds the potential to advance human knowledge in unimaginable ways, but we must remain fully aware of the risks associated with these advances. It is crucial that we begin preparing for these risks before they materialize into realities.

The telehealth.org website discusses the potential benefits that quantum computing brings to healthcare.

Quantum computing can benefit healthcare stakeholders by accelerating diagnoses, personalizing medicine, and optimizing pricing. It can be beneficial in :

- ***Diagnostics:*** *it facilitates early, accurate, and efficient computing of probable diagnoses and treatment outcomes.*
- ***Precision:*** *personalized interventions and treatments are identified for optimal health and disease management.*
- ***Pricing:*** *it can help to optimize insurance premiums and pricing and billing.*

More generally, it can speed the discovery of new treatments, creating greater effectiveness for manufacturers and greater efficiency for payers and healthcare providers. See IBM's Quantum Computing in Healthcare.

Dangers Ahead

Just as q-bits will be able to exist in two states at once, at the same time that quantum computing advances, it will also fundamentally increase cybersecurity risks, including being capable of breaking much of the public-key cryptography used on digital systems across the United States and around the world. This risk will allow malicious actors to easily decrypt encrypted data like passwords, personally

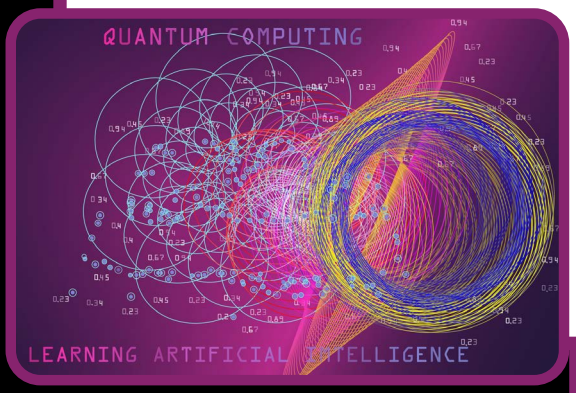
identifiable data, and personal health and financial information, making identity theft significantly more lucrative and easy to achieve. The risk that cyber criminals can steal data now and easily decrypt it when quantum computing becomes easily accessible, commonly known as "Harvest Now, Decrypt Later" or HNDL, means that protecting data now is even more important than ever.

That means some of the steps agencies can take now are the standard steps that security officers have advocated for years, such as taking an inventory of data and deciding how vulnerable it is and taking steps to mitigate any risk.

Looking Forward

The White House, Congress, and various government agencies have already started working to mitigate the threat posed by quantum computing.

- In May of 2022, President Biden signed the Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems, which outlines the administration's plan to address the cybersecurity risks posed by quantum computers. This plan includes requiring agencies to facilitate "a timely and equitable transition of the Nation's cryptographic systems to interoperable quantum resistant cryptography."
- The White House has also established a National Quantum Coordination Office, which coordinates and supports the National Quantum Initiative (NQI) including providing technical and administrative support to the National Science and Technology Council Subcommittee on Quantum Information Science and the National Quantum Initiative Advisory Committee and Overseeing interagency coordination of the NQI Program.
- In July, 2022, Congress passed the Quantum Computing Cybersecurity Preparedness Act, which requires government agencies to take steps to strengthen their cybersecurity efforts to prepare for quantum computing attacks.
- The Department of Homeland Security and the National Institute of Standards and Technology have formed a working group to help organizations protect their data and systems, and the Department of Health and Human Services has provided context and guidance for the health sector.



Quantum computing has the potential to advance human knowledge in ways we can only imagine, but we need to be fully aware of the risks those advances pose. We need to start preparing for those risks before they become realities.

If you have any questions about this newsletter or about cybersecurity at IHS, please feel free to contact Cybersecurity@ihs.gov.

NOTE: *The links in this document are for informational purposes only and do not signify an endorsement of any products contained within the linked sites/files.*