Quantum Computing: Global Threat or Way of the Future?

Chris Armour

University of Advancing Technology

SS320: Contemporary Global Issues

Professor David Brokaw

Have you ever wondered how safe the technology-driven society of the modern world really is? The vast ocean of data flowing around the world protected by simple lines of code. The computing power of technology increases year after year. Will these outdated standards stand the test of time? Enter quantum computing, the advancement in computing power that will determine the security of the future.

Quantum computing is a major leap forward in the computing power of the modern age. Currently, computer calculations and information can be broken down to their most basics of units called bits. “Ordinary computers store data and perform computations as a series of bits that are either 1 or 0” Overbye, 2019). The entirety of the digital world is stored in these simple on or off states. “By contrast, a quantum computer uses qubits, which can be 1 and 0 at the same time, at least until they are measured, at which point their states become defined” (Overbye, 2019). This seemingly simple addition of one state creates an almost infinite increase in computing power. It is because of this extreme increase in computing power, quantum computing will become a global threat.

The data of the world is protected by various forms of data encryption. Every time you visit a modern website such as Facebook, Amazon or, your bank, your data is being transmitted encrypted. “The encryption methods that are used today to transform data into an unreadable mush for anyone, but the intended recipients are essentially a huge maths problem” (Leprince-Ringuet, 2020). This is a great technology that gives the user an added reassurance that their data is secure from malicious hackers. The reason that these forms of encryption are secure is that normal computers are not capable of breaking the encryption in a useful time frame. This means

that the encryption algorithm is not unbreakable. Instead, it means that it will take months or even hundreds of years to break just one encrypted message.

The increase in computing power of the quantum computer will take these calculation times down to mere minutes. Modern encryption is measured quantified in terms of bits of security or the number of steps to break the encryption. A majority of the modern world is protected by 128-bit AES encryption. “It takes about 2,128 computational steps for an attacker to crack a 128-bit AES key” (Martin, 2017). It is essentially impossible with the non-quantum technology that will be available in the foreseeable future to crack a key that provides 128 bits of security. However, quantum computers would be able to break a 3,072-bit RSA key down to only 26-bits which would take the same computing power of a cellphone to break (Martin, 2017). Essentially, this would make all modern-day encryption algorithms obsolete giving access to the world’s data to malicious attackers.

This does not mean the end of the world quite yet, there is still hope. Billions of dollars are being invested in the research of Quantum technology by industry leaders such as Google and IBM, along with governments from around the world (Shankland, 2020). “As a direct result of the NSA's announcement five years ago, a global research effort into new quantum-safe cryptography protocols started in 2016, largely led by NIST in the US” (Leprince-Ringuet, 2020). There has already been over sixty-nine submissions to the project, of which fifteen are already showing promise. “The 15 algorithms selected by NIST this year are set to go through another round of review, after which the organization hopes to standardize some of the proposals. Before 2024, NIST plans to have set up the core of the first post-quantum cryptography standards” (Leprince-Ringuet, 2020). The modern world will have to put its faith

on the research of cryptography standards releases faster than the advancements of quantum computing.

In the end, the endless sea of data flowing across the world is safe for the time being. Steps are being taken to secure the future that is set to come. Do we still have to ask how long will the outdated encryption standards stand the test of time? The future of modern-day encryption sits waiting for its judgment from the quantum computing global threat.

References

Leprince-Ringuet, D. (2020, November 2). *Quantum computers could soon reveal all of our secrets. The race is on to stop that happening*. ZDNet. https://www.zdnet.com/article/quantum-computers-could-one-day-reveal-all-of-our-secrets/

Martin, L. (2017, November 16). *Is quantum computing the end of security as we know it?* TechBeacon. https://techbeacon.com/security/quantum-computing-end-security-we-know-it

Overbye, D. (2019, October 23). *Quantum computing is coming, bit by Qubit*. The New York Times. https://www.nytimes.com/2019/10/21/science/quantum-computer-physics-qubits.html

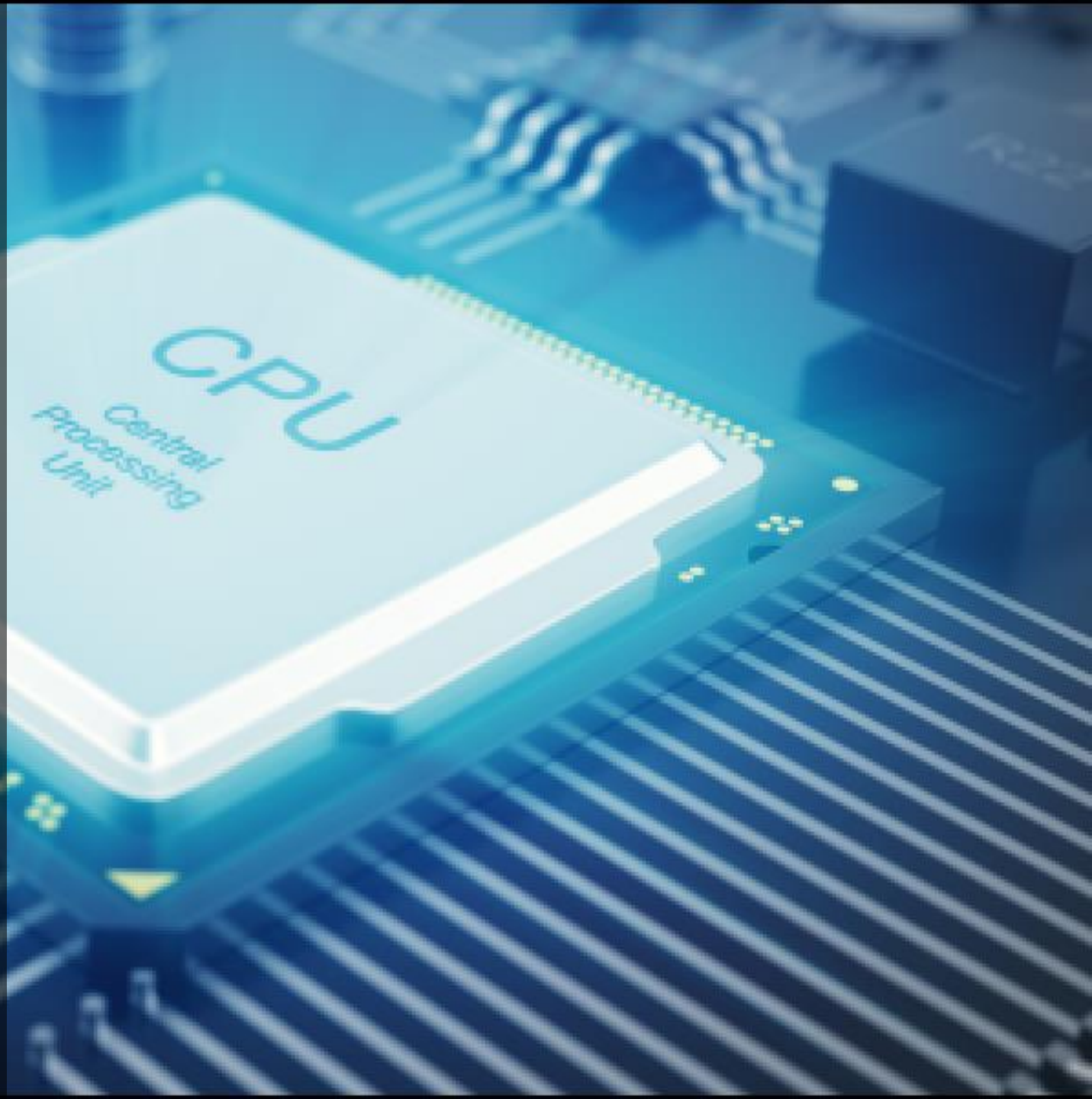
Shankland, S. (2020, August 26). *With $1 billion in quantum computing research, the US hopes to outpace 'adversaries'*. CNET. https://www.cnet.com/news/us-begins-1-billion-quantum-computing-plan-to-get-ahead-of-adversaries/

Quantum Computing: Global Threat or Way of the Future?

Created by: Chris Armour
University of Advancing Technology
SS320: Contemporary Global Issues

Modern Computing

- Information stored in bits
  - 1s and 0s
- Electrically stored Either on or off
- Data Steamed in order
- Data changed by voltage
- Usage of Central Processing Unit



Quantum Computing

- Information stored in Qubits
  - 1s, 0s or Both
- More than on State at a time
- Data changed at electron/Photon level
- Uses Quantum Processing Unit with connected Qubits

Global Threat

- Modern 128-bit Encryption
- Not unbreakable
- Security based on time
- Classical Computing
  - Near impossible to crack
  - Hundreds of Years
- Quantum Computing
  - Less than 24 hours to crack
  - Can reduces 3,072-bit RSA key to 26-bits

Future Hope: Post-Quantum Cryptography

- Government and Industry Researchers
- Goal: Encryption that can withstand Quantum Computing
- NIST 69 Algorithm Candidates
  - 15 viable for future development
- NIST 2024 Core Post-Quantum Standard

Q & A

References

- How To Geek. (n.d.). [Digital Media]. How To Geek. https://www.howtogeek.com/wp-content/uploads/2018/10/cpu_lede.png
- IBM. (n.d.). *IBM System one* [Photograph]. IBM. https://www.ibm.com/quantum-computing/
- Leprince-Ringuet, D. (2020, November 2). *Quantum computers could soon reveal all of our secrets. The race is on to stop that happening*. ZDNet. https://www.zdnet.com/article/quantum-computers-could-one-day-reveal-all-of-our-secrets/
- Martin, L. (2017, November 16). *Is quantum computing the end of security as we know it?* TechBeacon. https://techbeacon.com/security/quantum-computing-end-security-we-know-it
- Medium. (n.d.). [Digital Media]. Medium. https://medium.com/searchencrypt/what-is-encryption-how-does-it-work-e8f20e340537
- Overbye, D. (2019, October 23). *Quantum computing is coming, bit by Qubit*. The New York Times. https://www.nytimes.com/2019/10/21/science/quantum-computer-physics-qubits.html
- Shankland, S. (2020, August 26). *With $1 billion in quantum computing research, the US hopes to outpace 'adversaries'*. CNET. https://www.cnet.com/news/us-begins-1-billion-quantum-computing-plan-to-get-ahead-of-adversaries/