Post-Quantum Cryptography

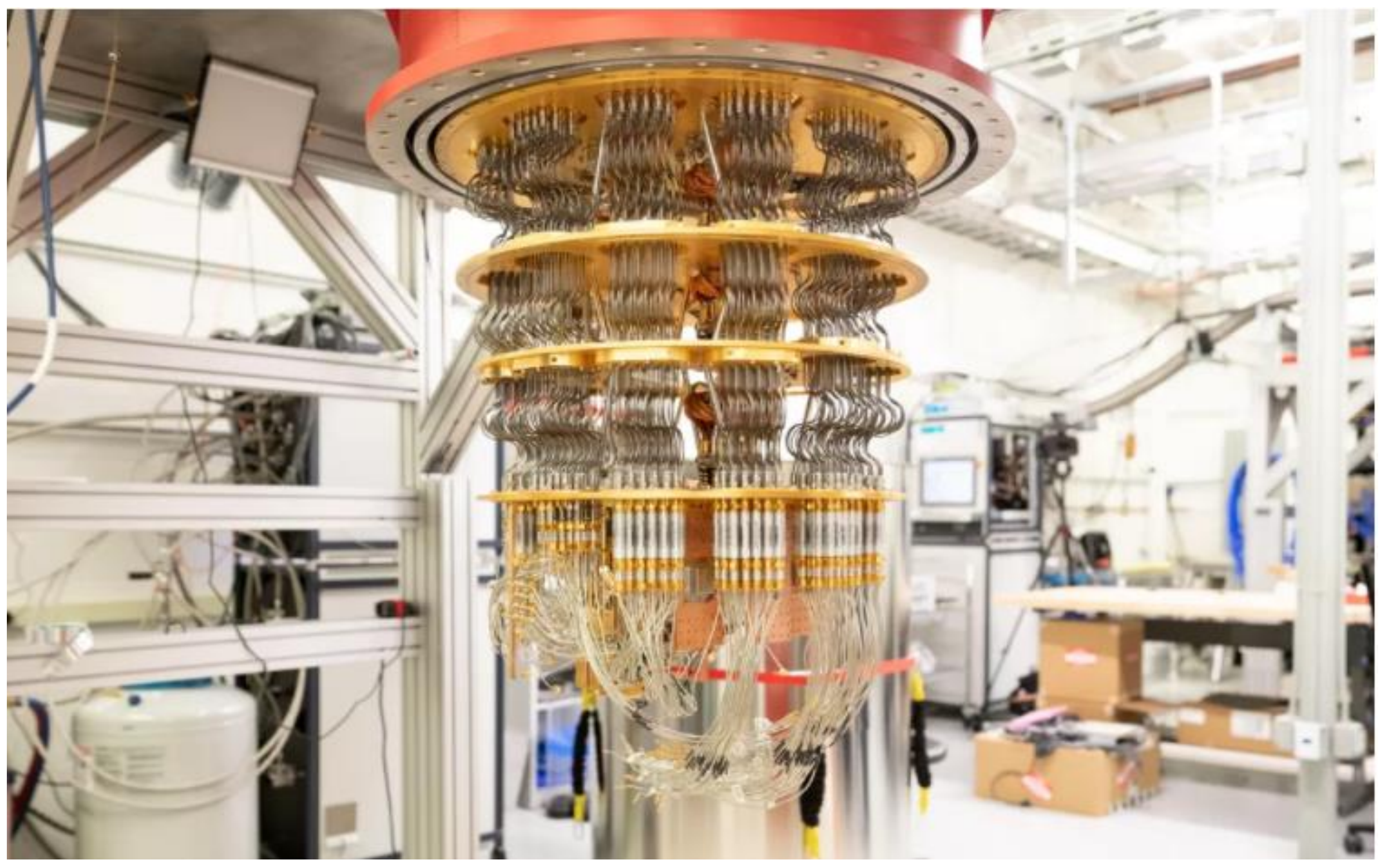
Team: Danica Cariaga, Amber Thomas
College of Science, Computer Science
College of Engineering, Electrical and Computer Engineering
Cal Poly Pomona Cybersecurity and Awareness Fair 2021
Problem-Solving Category

Problem

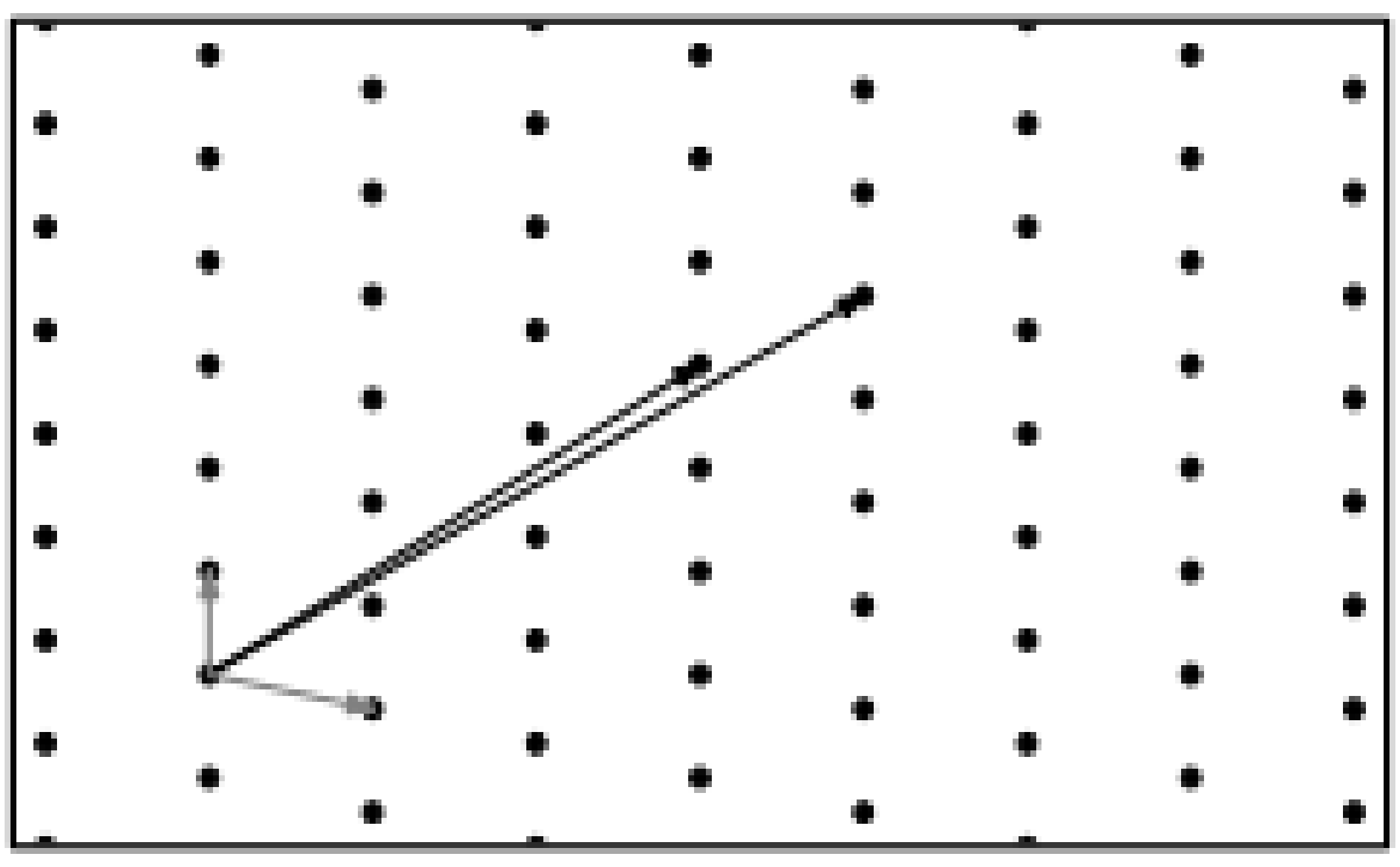
- Quantum computers (QC) are on track to break our current encryption algorithms
- Strong encryption standards is necessary to protect data
- QC cracking algorithms, private data will be exposed
- RSA crack – conventional computer vs. QC

Analysis

- Processing times for bits vs. qubits
- Lattice-based cryptography
  - Shortest Vector Problem (SVP)
- Distributed web-systems
- NIST Post-Quantum Cryptography future standardization



Shankland, Stephen. "Google plans to make million-qubit quantum computers by 2029 that are much more powerful than this system it showed in 2019" CNET, 24 May 2021, https://www.cnet.com/tech/computing/quantum-computers-could-crack-todays-encrypted-messages-thats-a-problem/



Micciancio, Daniele. "**Figure 1.** A two-dimensional lattice and two possible bases" NYU-CIMS, 22 July 2008, https://cims.nyu.edu/~regev/papers/pqc.pdf

Challenges

- Shor's Algorithm
- Harvest data-collect now, crack later
- Migration time

Recommendations

- Implement migration now
- Post-quantum protocols developed with quantum key distributions
- Research and collaboration with existing infrastructure and researchers

Sources

•Asif, Rameez. "Basic types of Post-Quantum Cryptography (PQC)" MDPI, 5 Feb. 2021, https://www.mdpi.com/2624-831X/2/1/5/htm
•Barker, William, and Murugiah Souppaya. “Migration to Post-Quantum - Nccoe.org.” National Cybersecurity Center of Excellence (NCCoE), https://www.nccoe.org/sites/default/files/library/project-descriptions/pqc-migration-project-description-final.pdf.
•Campagna M., LaMacchia B., & Ott D. (2020) Post Quantum Cryptography: Readiness Challenges and the Approaching Storm. https://cra.org/ccc/resources/ccc-led-whitepapers/#2020-quadrennial-papers
•Computer Security Division, Information Technology Laboratory. “Post-Quantum Cryptography: CSRC.” CSRC, 14 June 2021, https://csrc.nist.gov/Projects/Post-Quantum-Cryptography.
•“Cryptography in a Post- Quantum World - Accenture.” Accenture, 4 Oct. 2018, https://www.accenture.com/_acnmedia/pdf-87/accenture-809668-quantum-cryptography-whitepaper-v05.pdf.
•Micciancio, Daniele, and Oded Regev. “Lattice-Based Cryptography.” *NYU CIMS*, 22 July 2008, https://cims.nyu.edu/~regev/papers/pqc.pdf.
•Nassief, Andrew M. K. “Distributed Web Systems Leading to Hardware Oriented Cryptography and Post-Quantum Cryptologic Methodologies.” IACR Cryptology EPrint, 14 Dec. 2019, https://www.academia.edu/41405212/Distributed_Web_Systems_Leading_to_Hardware_Oriented_Cryptography_an_Post_Quantum_Cryptologic_Methodologies.
•“NSAs Cybersecurity Perspective on Post Quantum Cryptography Algorithms.” National Security Agency/Central Security Service > Cybersecurity > https://www.nsa.gov/Cybersecurity/NSAs-Cybersecurity-Perspective-on-Post-Quantum-Cryptography-Algorithms/.
•Shankland, Stephen. “Quantum Computers Could Crack Today's Encrypted Messages. That's a Problem.” CNET, CNET, 24 May 2021, https://www.cnet.com/tech/computing/quantum-computers-could-crack-todays-encrypted-messages-thats-a-problem/.
•Staff, NQCO. “NSA Updates FAQ on Post-Quantum Cybersecurity.” National Quantum Initiative, 10 Aug. 2021, https://www.quantum.gov/nsa-updates-faq-on-post-quantum-cybersecurity/.