The Next Frontier in Hardware Security: Quantum Computers

Prof. Jakub Szefer

Computer Architecture and Security Lab

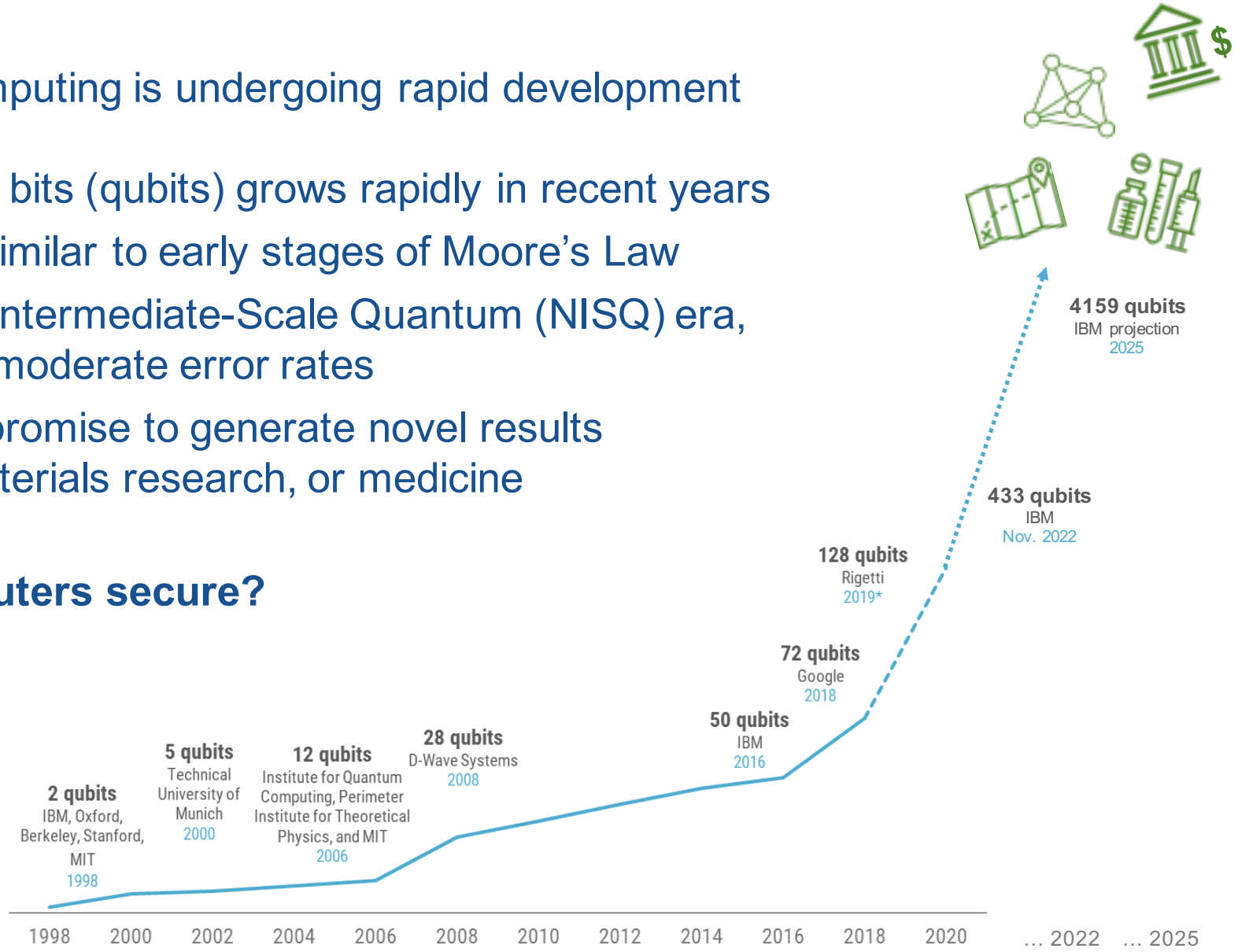
https://caslab.io

Quantum Computers Can Solve New Problems

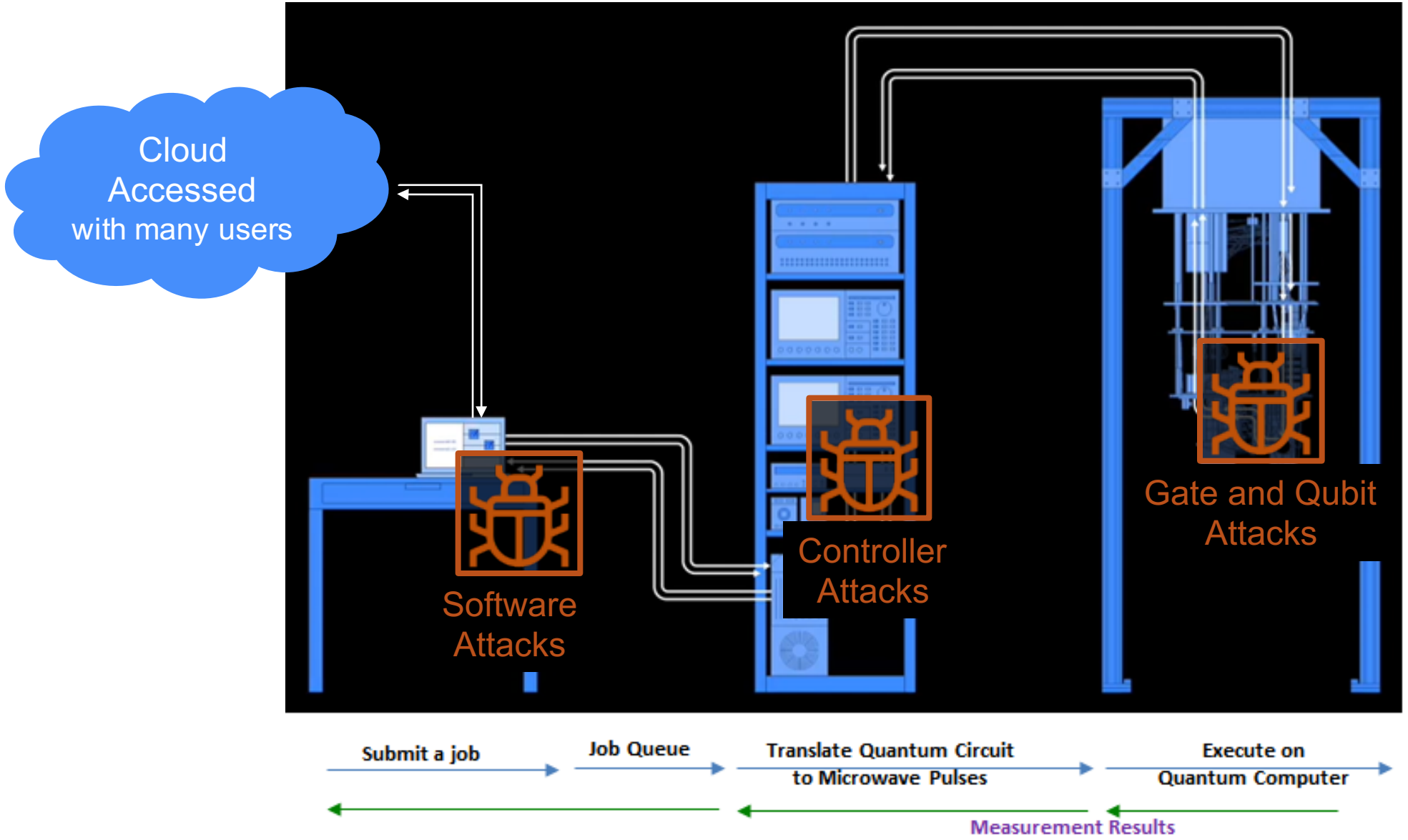
The field of quantum computing is undergoing rapid development

- Number n of quantum bits (qubits) grows rapidly in recent years
- Development trends similar to early stages of Moore's Law
- Current stage: Noisy Intermediate-Scale Quantum (NISQ) era, 10^1 to 10^2 qubits and moderate error rates
- Quantum computers promise to generate novel results in, e.g., chemistry, materials research, or medicine

But are quantum computers secure?



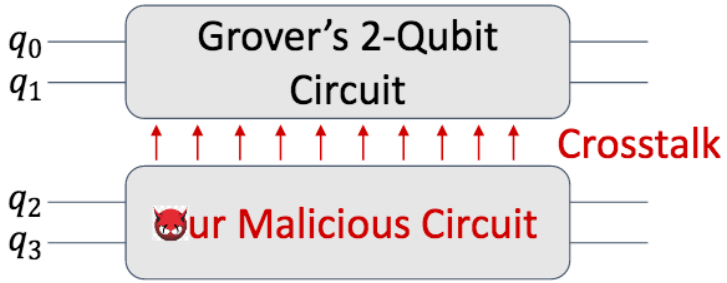
Where can Quantum Computers be Vulnerable?

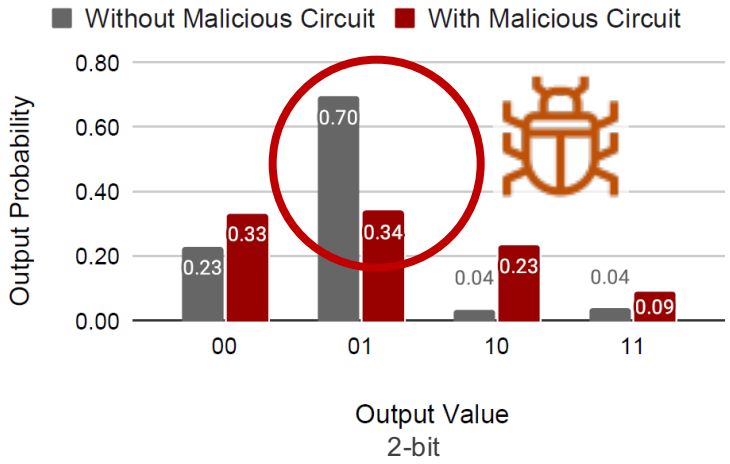


Yale

Software Attacks

- Users can submit circuits to execute, with no security checks today
- Sharing of quantum computers will facilitate more attacks
  - Single-tenant model, today
  - Multi-tenant model, proposed
- Possible **circuit virus attacks**

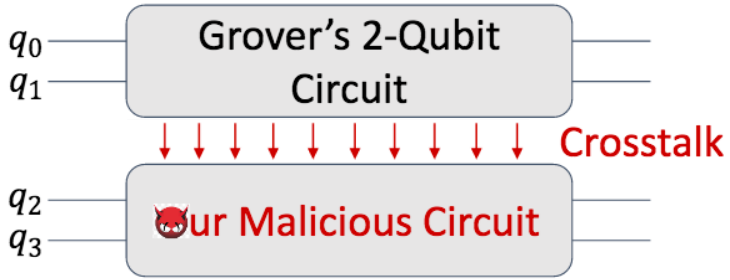




Yale

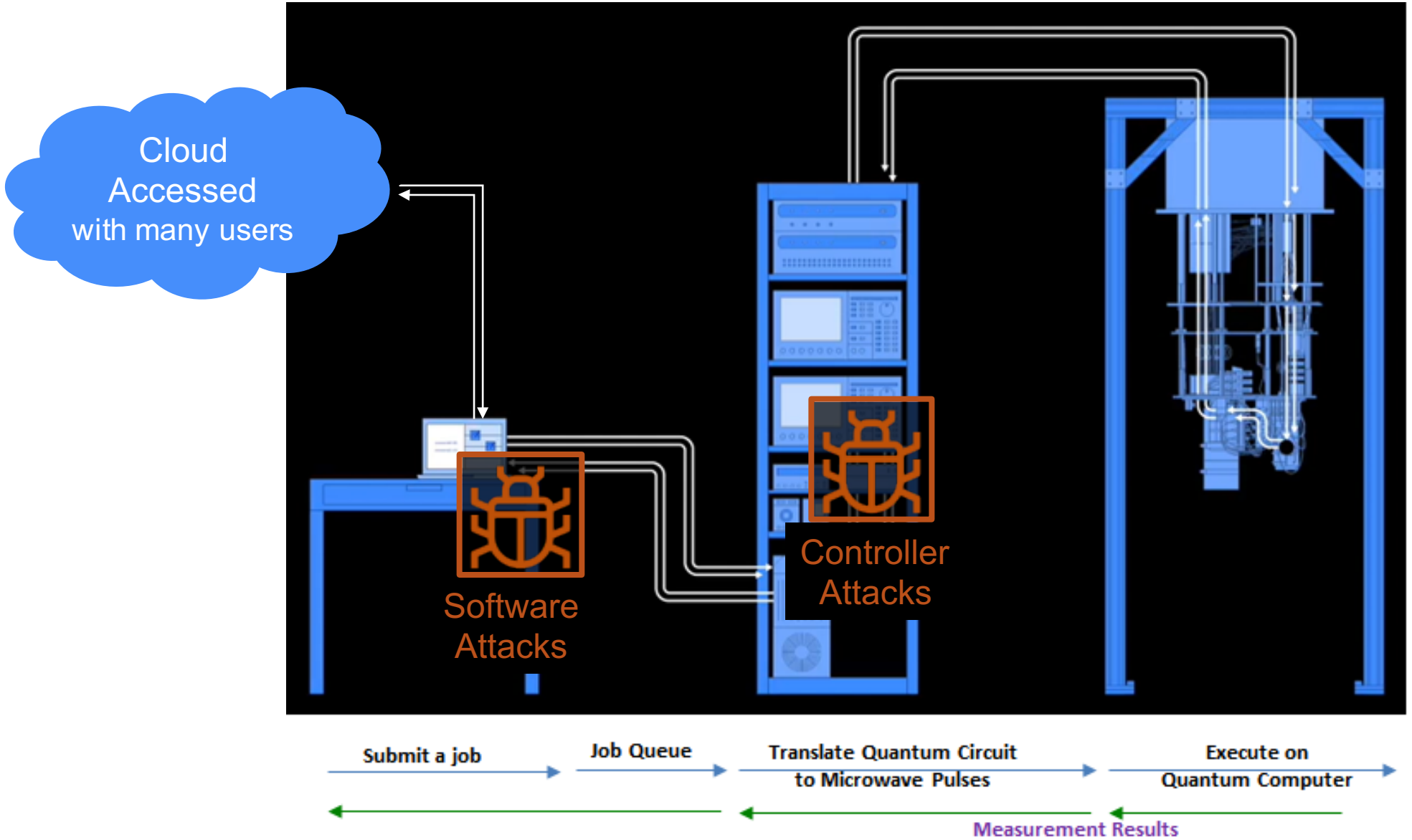
Software Attacks

- Users can submit circuits to execute, with no security checks today
- Sharing of quantum computers will facilitate more attacks
  - Single-tenant model, today
  - Multi-tenant model, proposed
- Possible **circuit spy attacks**



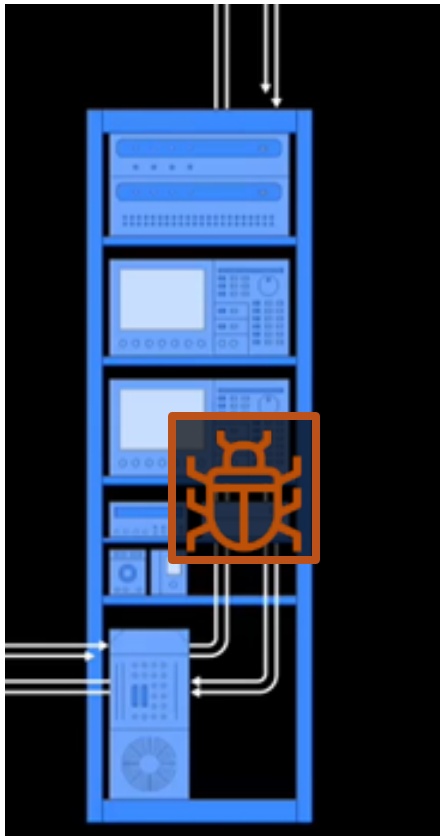
Yale

Where can Quantum Computers be Vulnerable?

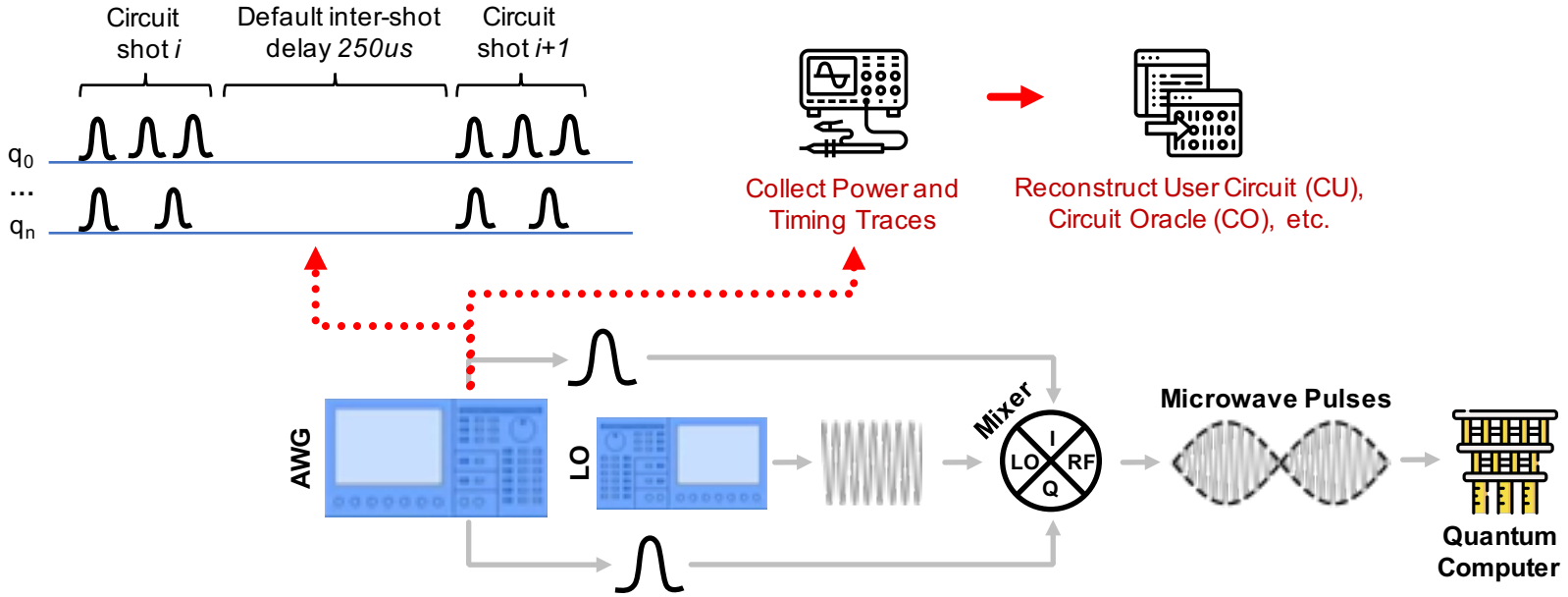


Yale

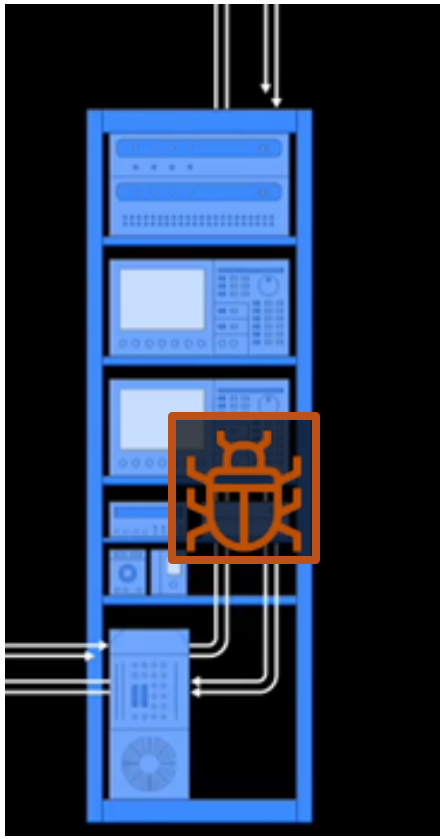
Controller Attacks



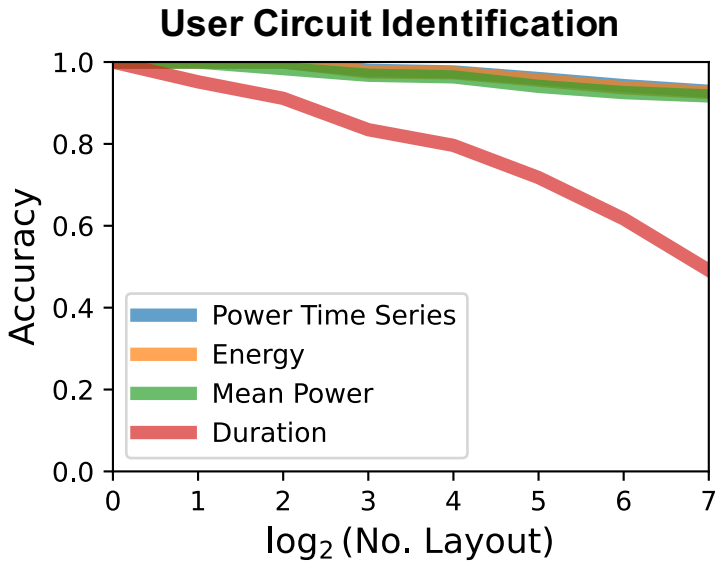
- Quantum computers use extensive set of hardware for controlling the qubits
- Users have no control over remote quantum computers
  - Honest-but-curious cloud provider
  - Malicious insiders
- Possible timing and **power side-channel attacks**



Controller Attacks

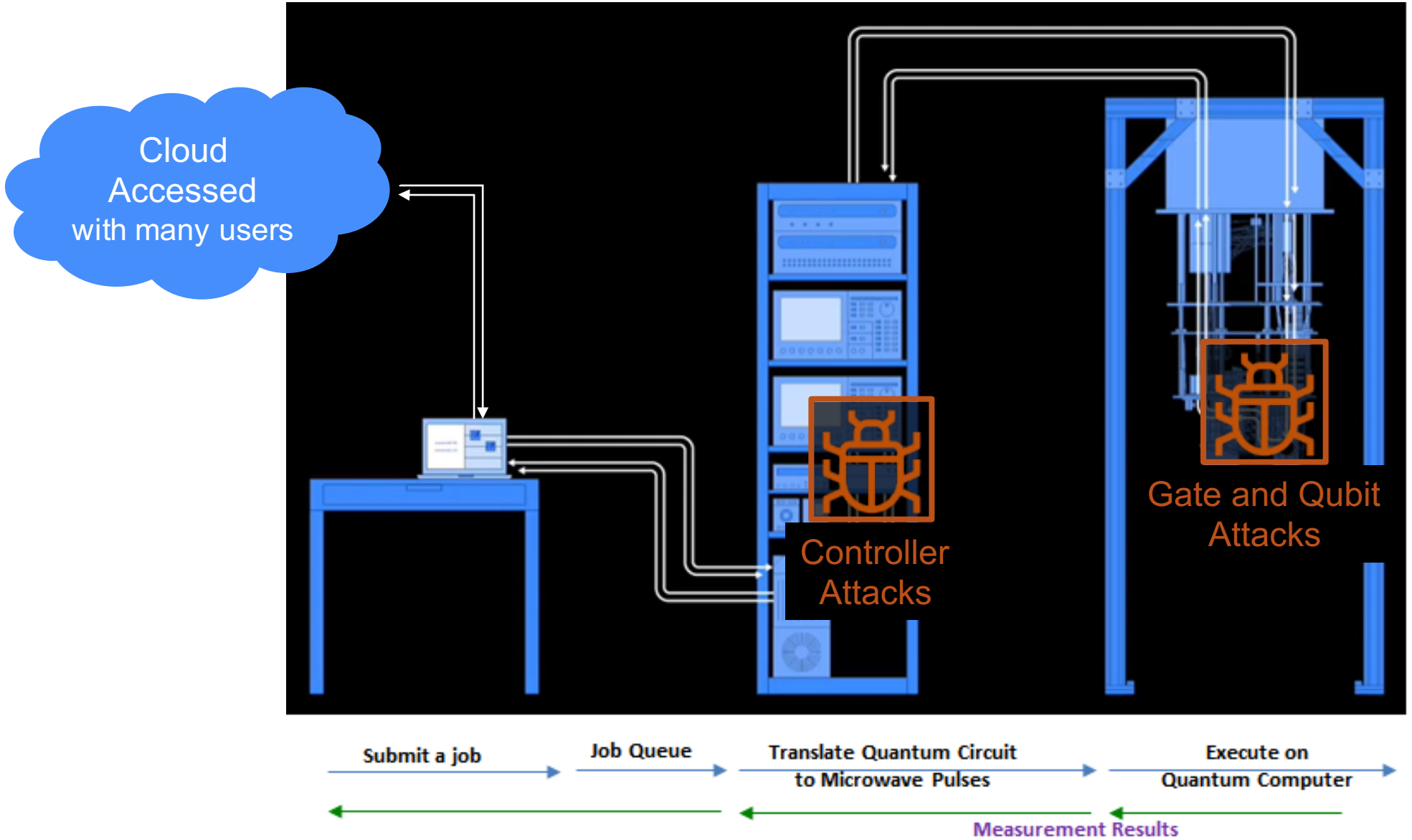


- Quantum computers use extensive set of hardware for controlling the qubits
- Users have no control over remote quantum computers
  - Honest-but-curious cloud provider
  - Malicious insiders
- Possible timing and **power side-channel attacks**
  - (UC) User Circuit Identification
  - (CO) Circuit Oracle Identification
  - (CA) Circuit Ansatz Identification
  - (QM) Qubit Mapping Identification
  - (QP) Quantum Processor Identification
  - (RP) Reconstruction from Power Traces



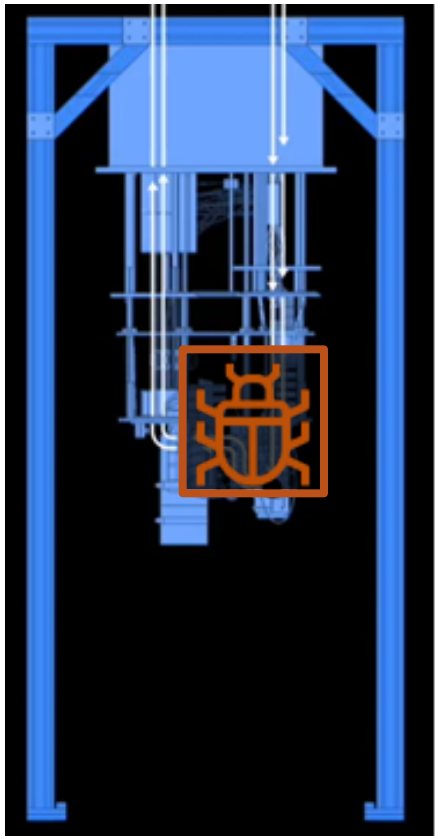
Yale

Where can Quantum Computers be Vulnerable?



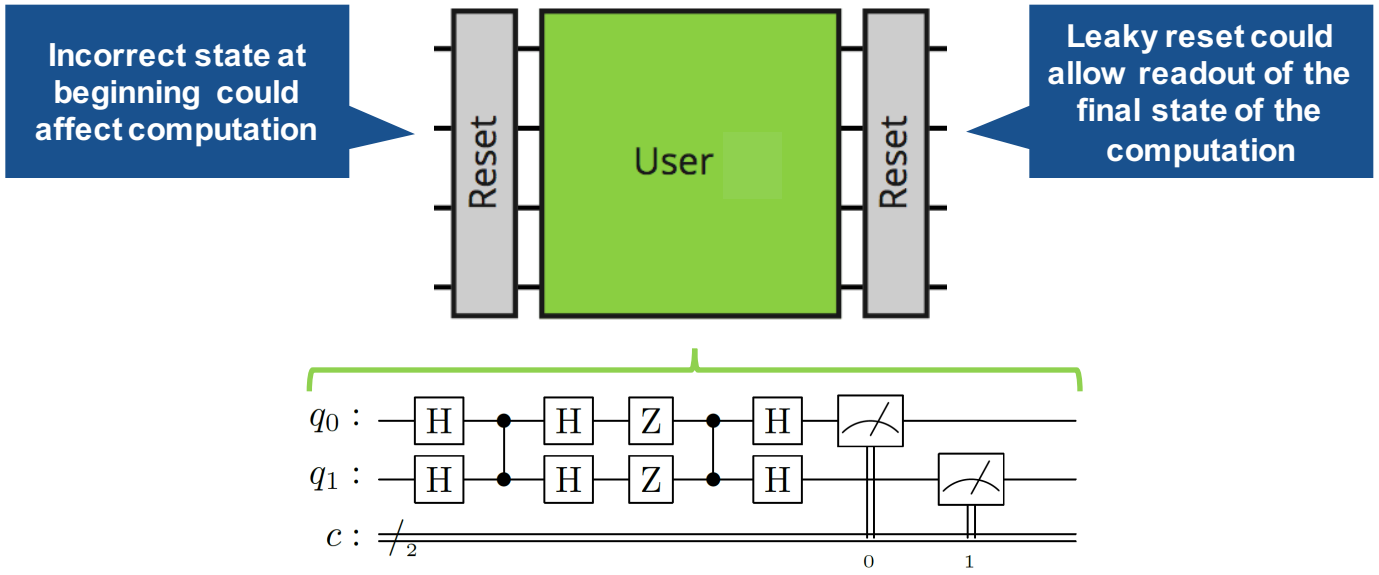
Yale

Gate and Qubit Attacks



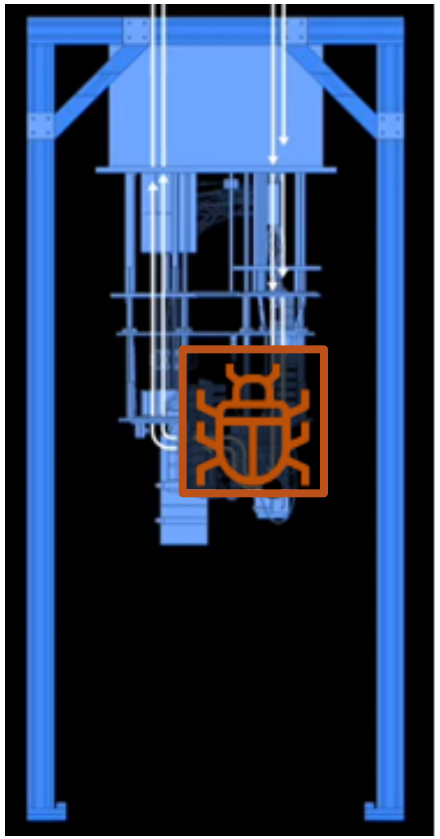
- Imperfections in physical qubit and gate operations of quantum computers can be abused by attackers
  - Physical noise, crosstalk
  - Imperfect operations, measurement errors
  - Etc.

- Imperfections in operation lead to **information leaks**



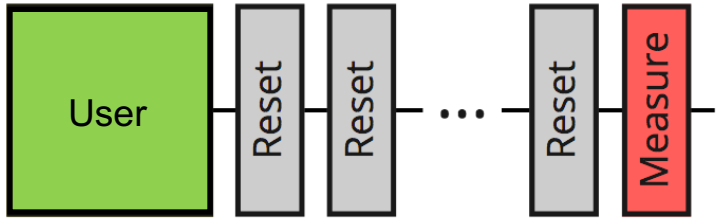
Yale

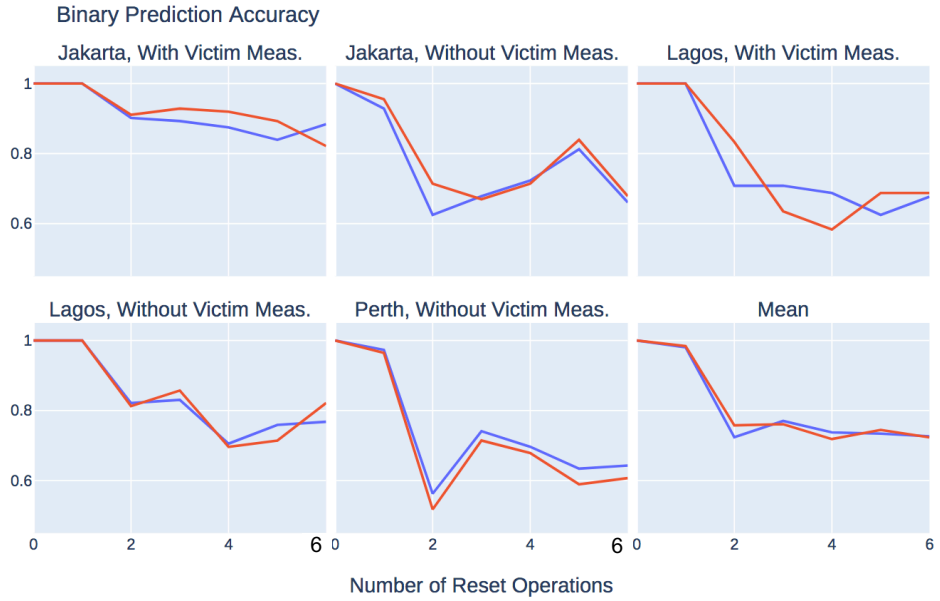
Gate and Qubit Attacks



- Imperfections in physical qubit and gate operations of quantum computers can be abused by attackers

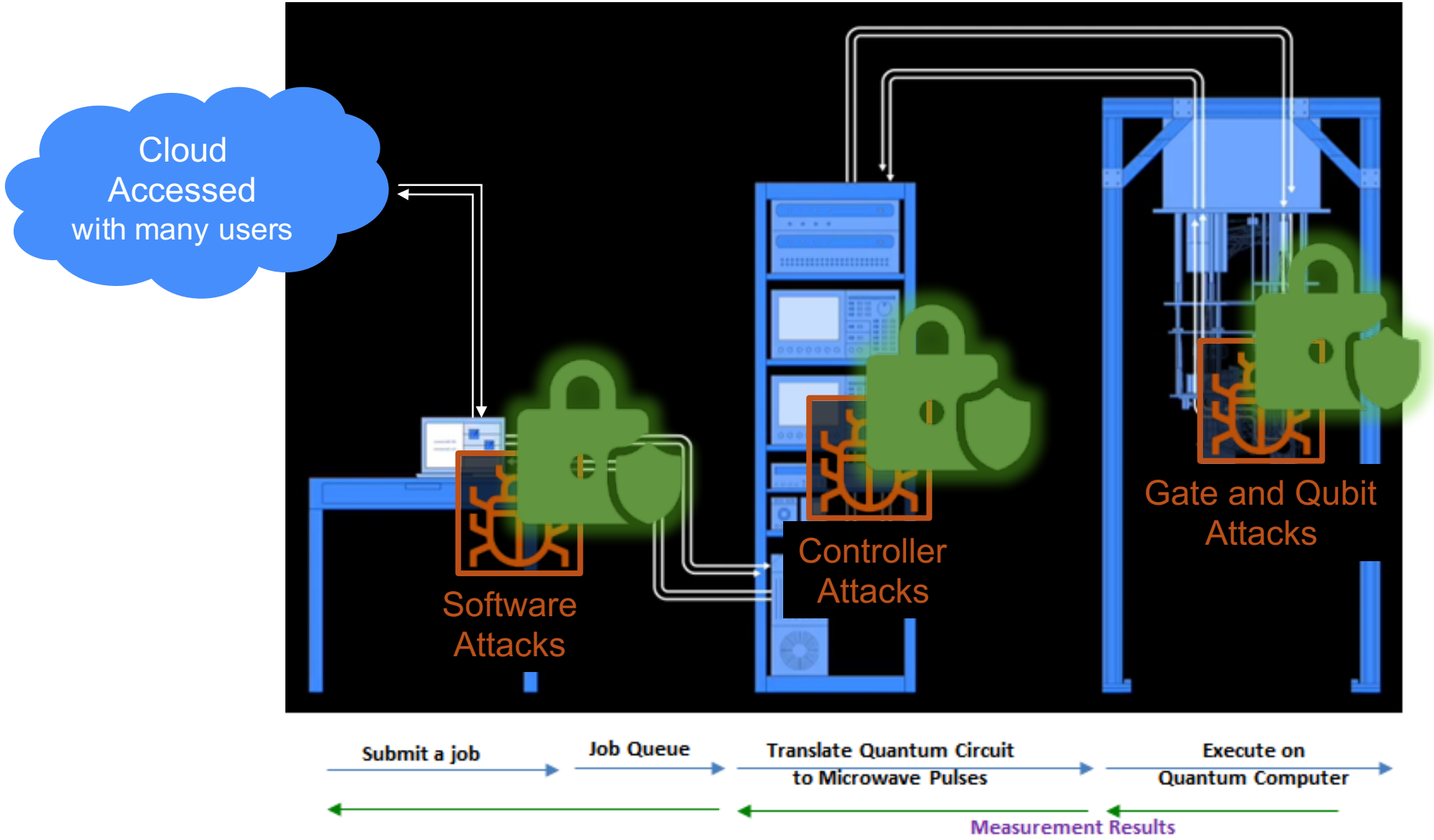
- Example **reset gate information leak**
  - Build model that infers $|\Psi\rangle$ given measurement m and number of resets r which have occurred
  - Prediction accuracy of $\theta \in \{0, \pi\}$, i.e. qubit states that approximate $|0\rangle$ or $|1\rangle$





Yale

Next Frontier: Quantum Computer Security

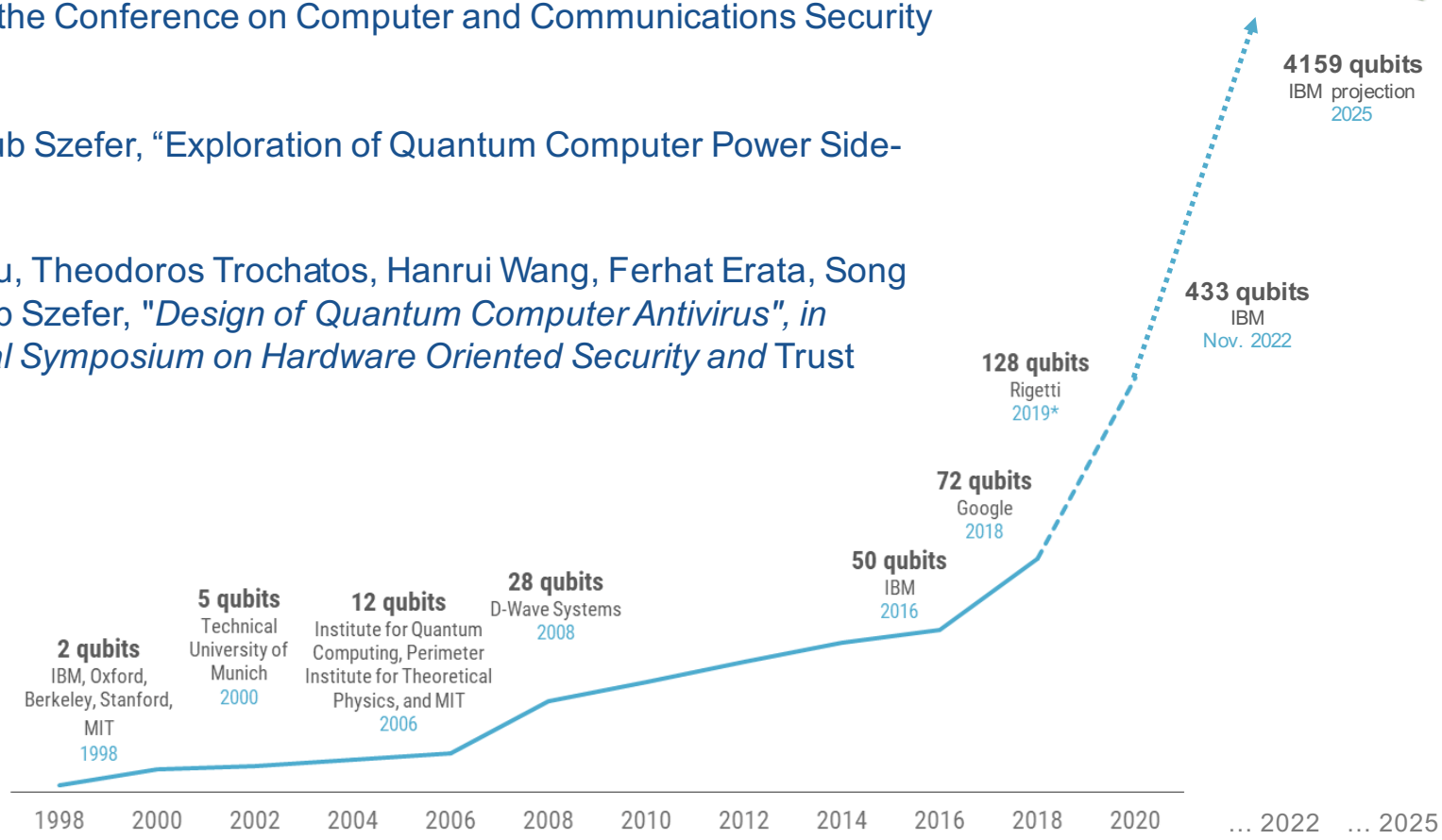


Yale

Next Frontier: Quantum Computer Security

The field of quantum computing is undergoing rapid development and concurrently **we need to design secure quantum computers**.

- Allen Mi, Shuwen Deng, and Jakub Szefer, "*Securing Reset Operations in NISQ Quantum Computers*", in Proceedings of the Conference on Computer and Communications Security (CCS), November 2022.
- Chuanqi Xu, Ferhat Erata, Jakub Szefer, “Exploration of Quantum Computer Power Side-Channels”, arXiv, April 2023.
- Sanjay Deshpande, Chuanqi Xu, Theodoros Trochatos, Hanrui Wang, Ferhat Erata, Song Han, Yongshan Ding, and Jakub Szefer, "*Design of Quantum Computer Antivirus", in Proceedings of the International Symposium on Hardware Oriented Security and* Trust (HOST), May 2023.



Thanks!

Prof. Jakub Szefer

Computer Architecture and Security Lab

https://caslab.io