Quantum Computer Hardware Cybersecurity

Computer Architecture and Security Laboratory @ Yale

Prof. Jakub Szefer
Dept. of Electrical Engineering
Yale University

https://caslab.csl.yale.edu/~jakub

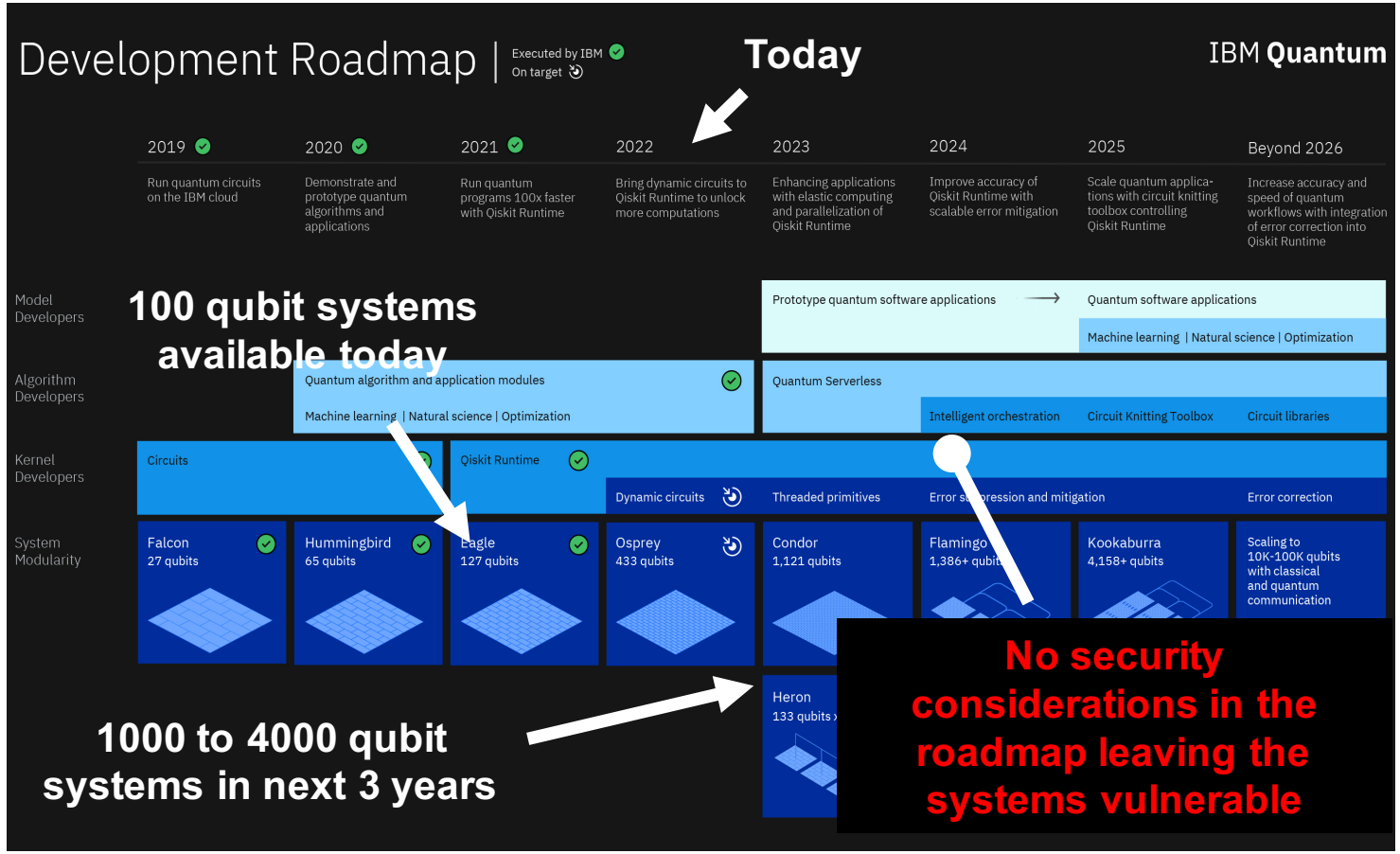
Quantum Computers Today

Quantum computer advances are presented every year with bigger and bigger machines coming online

- 100+ qubit systems are available today as pay-per-use cloud devices from IBM, and others are also building quantum computer clouds, for example, Amazon Braket or Microsoft Azure

Quantum computers can facilitate novel discoveries

- Quantum computers are not general-purpose computers but can generate valuable and sensitive intellectual property
- Design of the computers itself may be sensitive or secret



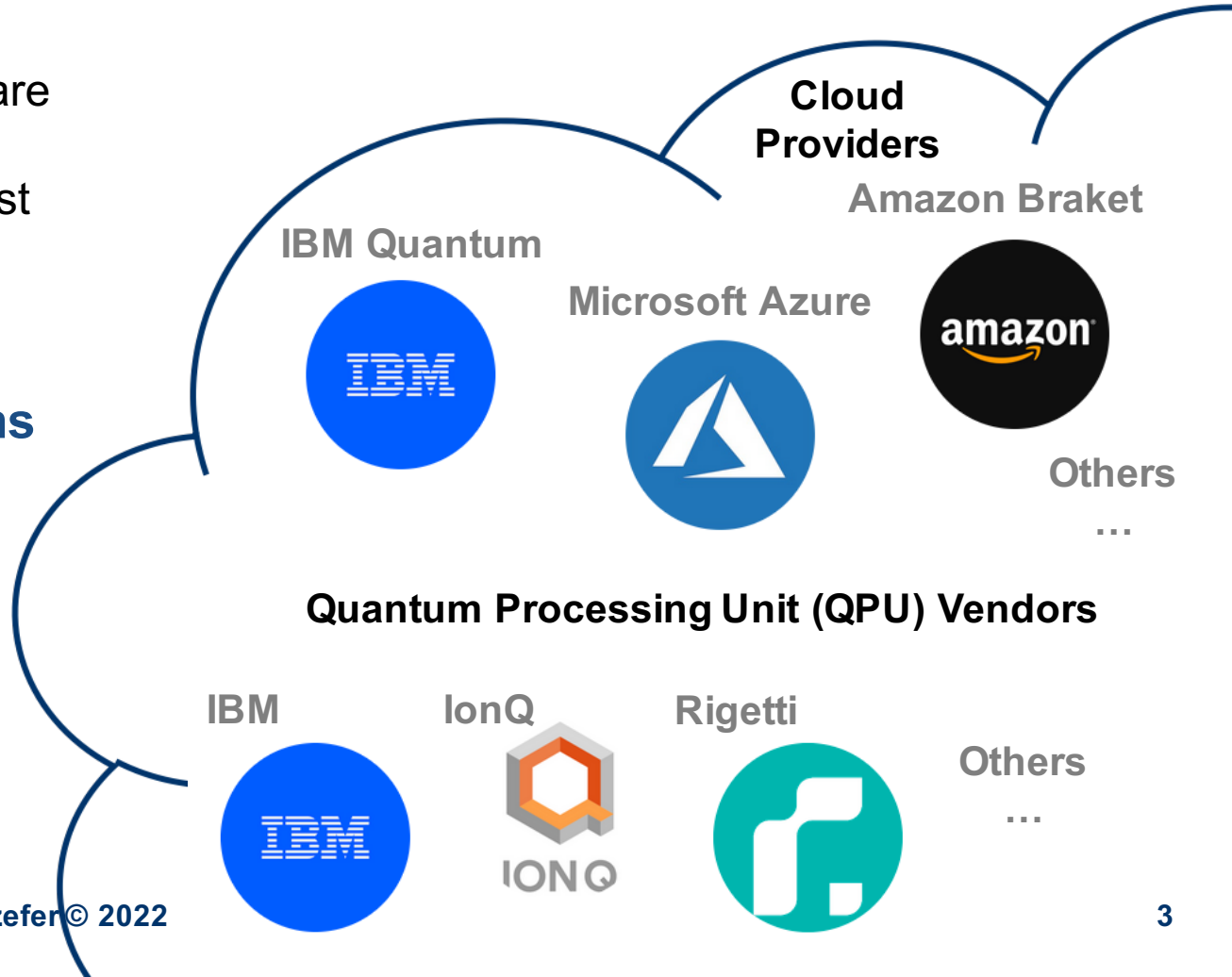
Quantum Computing as a Service (QCaaS)

Quantum Computers are rapidly being deployed as cloud-based accelerators today

- Size is still very limited ~100 qubits
- But can relatively easily experiment with hardware through cloud-based access
- Free and paid cloud-based services already exist
- Many companies are pushing for Quantum Computer as a Service (QCaaS) deployments

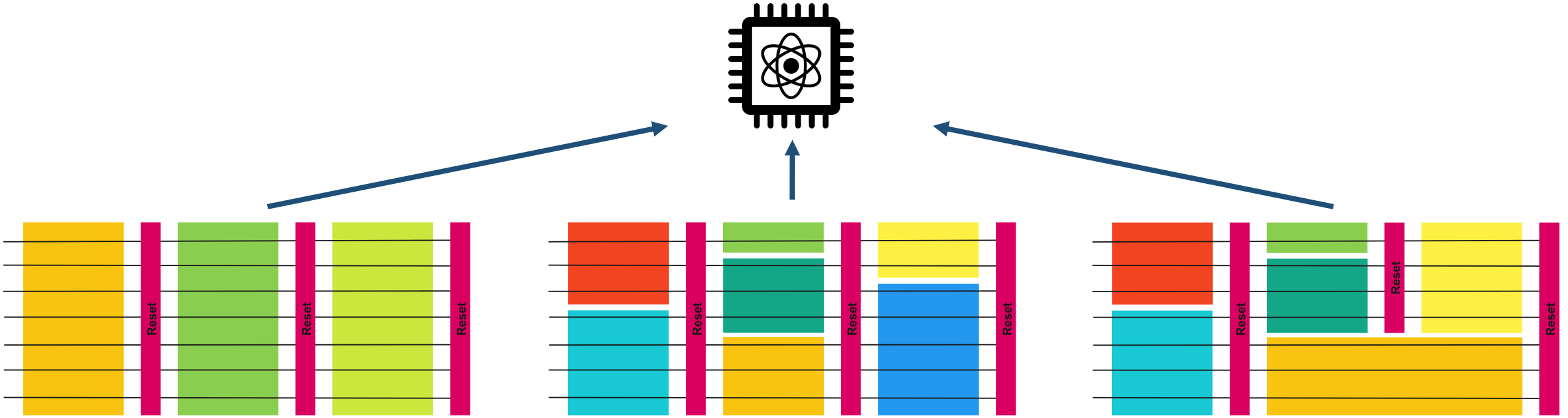
But there are few or no security considerations in QCaaS today

- Possibly malicious users can now access quantum computing hardware remotely
- Very few if no security checks, like early days of cloud computing or cloud-based FPGAs



Spatial and Temporal Sharing of Qubits in QCaaS Setting

Quantum computer's qubits can be shared among programs or users in different ways:



- Single-tenant, execute one user or program at a time

Today

- Multi-tenant, execute multiple programs or users in batches

Future

- Multi-tenant, execute multiple programs or users

Future

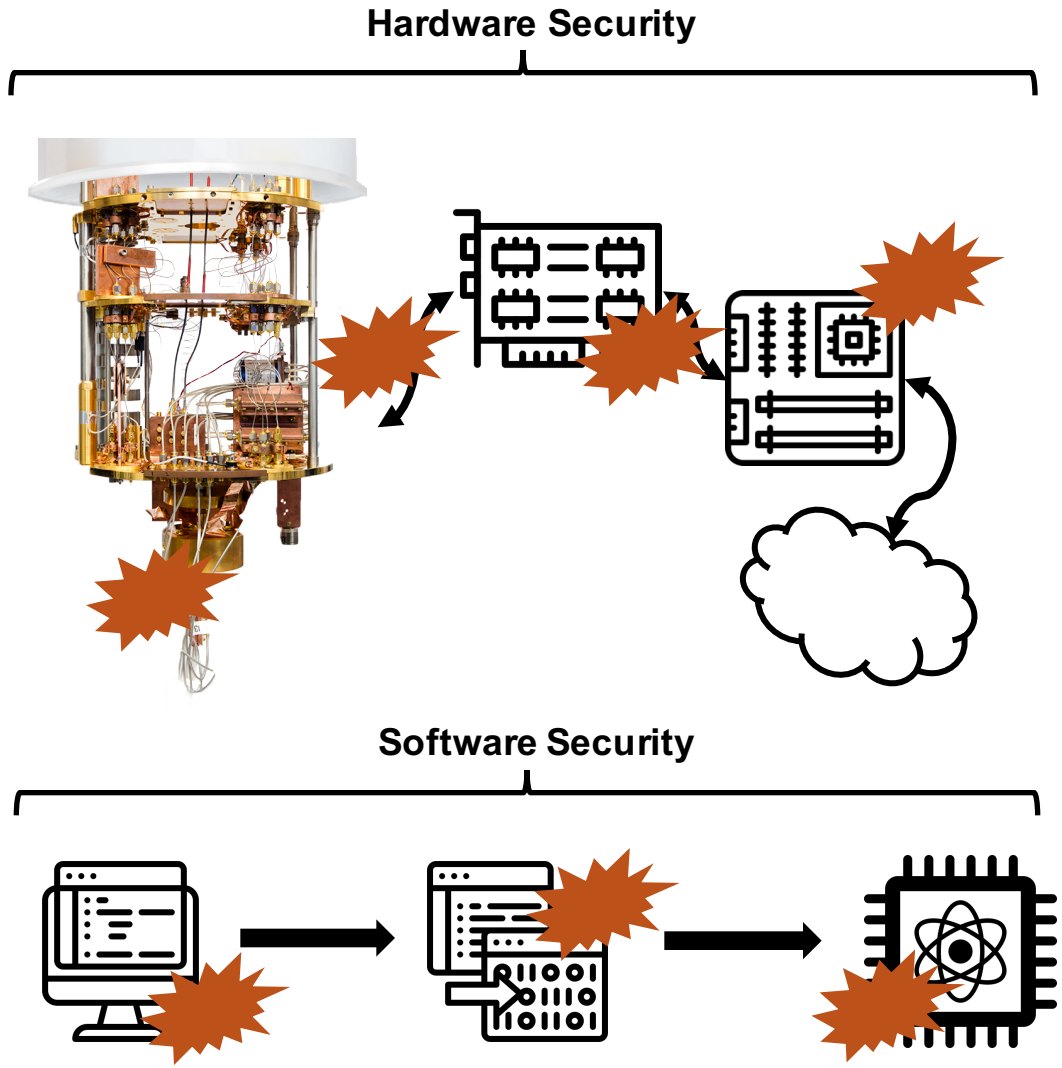
Security Threats to Quantum Computers

Hardware security:

- Are there ways to protect the hardware so that it cannot be reverse engineered?
- Is it possible to reverse engineer a cloud-based quantum computer by running various quantum circuits, and if so, are protections possible?
- What physical attacks are possible to disturb operation of quantum computers, or to leak information from them?

Software security:

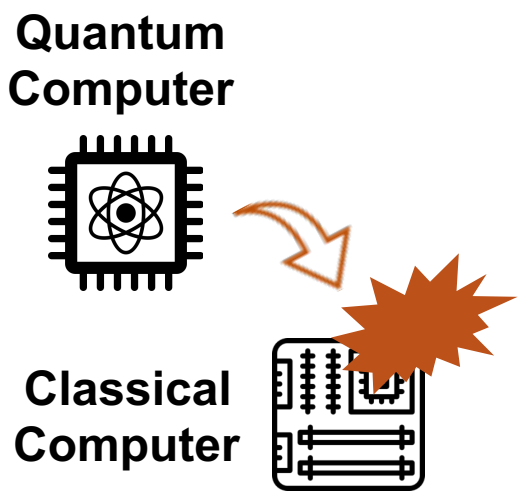
- Is there a way to detect or prevent a user from running certain algorithms on a cloud-based quantum computer?
- What are the cybersecurity threats that are different between classical and quantum computing systems?



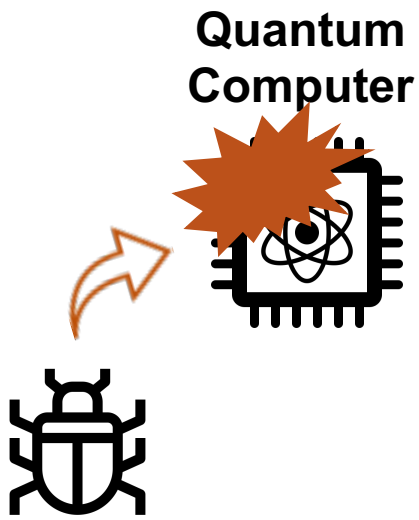
Unexplored Side of Quantum Computer Security

Others → **Us** → **Talk Outline**

Almost all of existing quantum computer security research focuses on attacks using the computers to break classical cryptography



Our research focuses on protecting quantum computers from security attacks to protect the algorithms and data on quantum computers



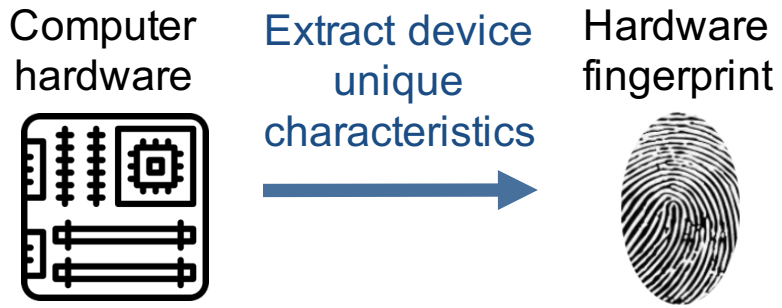
- Fingerprinting Quantum Computers
- Fingerprinting Quantum Computer Infrastructures
- Information Leaks Across Reset Gates
- Toward Software Defense of Quantum Computers
- Physical Attacks on Quantum Computers

Fingerprinting Quantum Computers

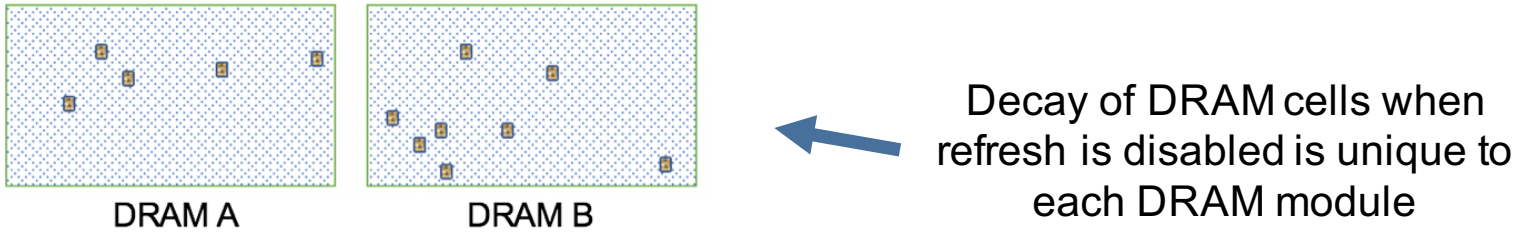
Computer Hardware Fingerprinting

Fingerprinting of computer hardware is used to uniquely identify a piece of computer hardware

- Usually based on some analog feature(s) of the hardware
- Using features affected by manufacturing variations
- Assuming the features are hard to duplicate exactly



Classical computer example:
DRAM-based Physical Unclonable Functions (PUF)

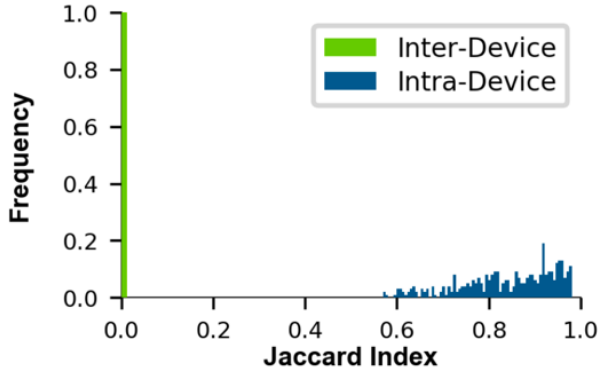


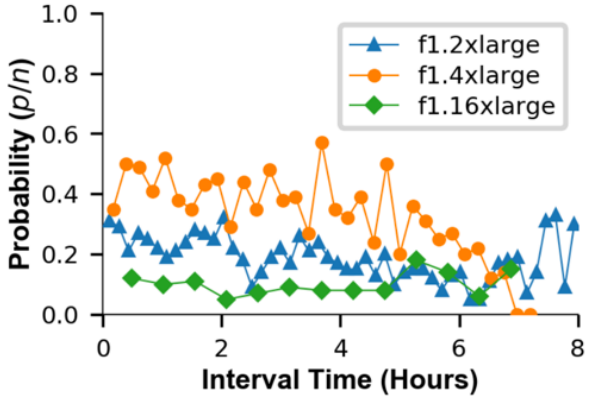
- Fingerprint is the set of DRAM cells that decay after some time *t*
- Use Jaccard index as metric to decide if fingerprint is from same or different device

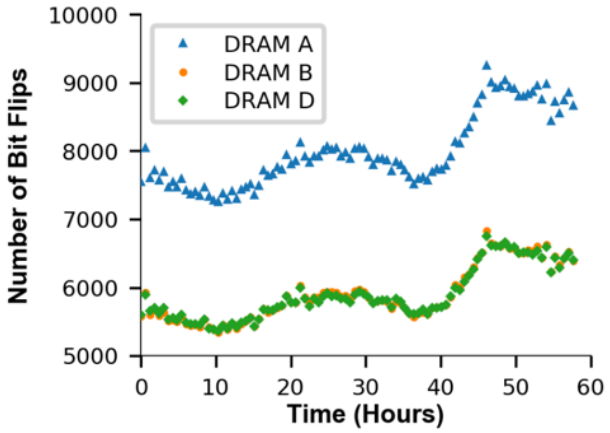
Example Security Implications of Hardware Fingerprinting

Examples from our work on fingerprinting cloud-based FPGAs:

- Fingerprinting can reliably distinguish FPGAs based on the DRAM PUFs
  - Inter- and intra-device Jaccard Index shows clear separation of the fingerprints
- Can learn probability of getting same FPGA instance over time
  - Insights into allocation algorithm
- Can monitor data center temperature remotely through DRAM decay rates
  - Fluctuations for different times of day or week days





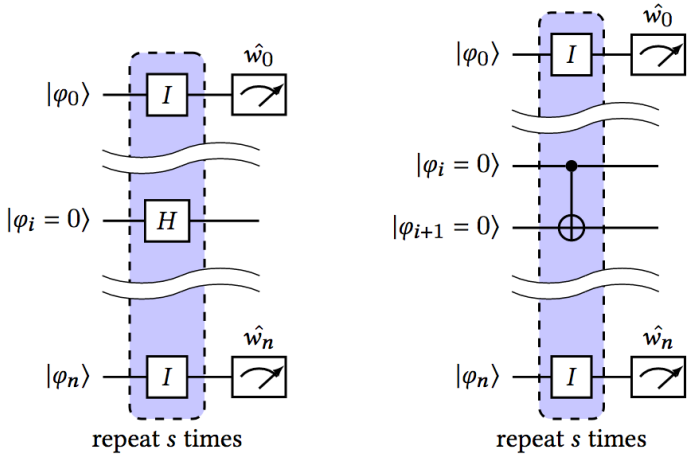


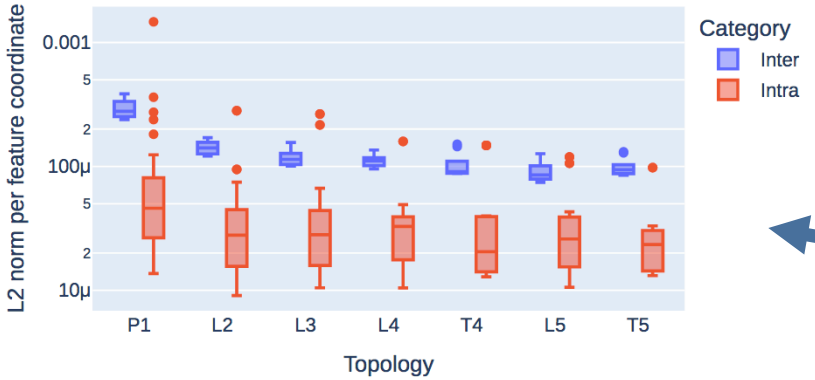
Quantum Computer Fingerprinting

First idea, gate and other errors depend in part on manufacturing variations, can these be leveraged as source of a fingerprint?

Idle Tomography (IDT) based fingerprinting approach:

- IDT is used to characterize crosstalk error rates
- But can use IDT to also find device-specific patterns in crosstalk
- The error rates for the different qubits constitute the fingerprint





Distributions of inter- and intra-embedding separation for various topologies across all batches

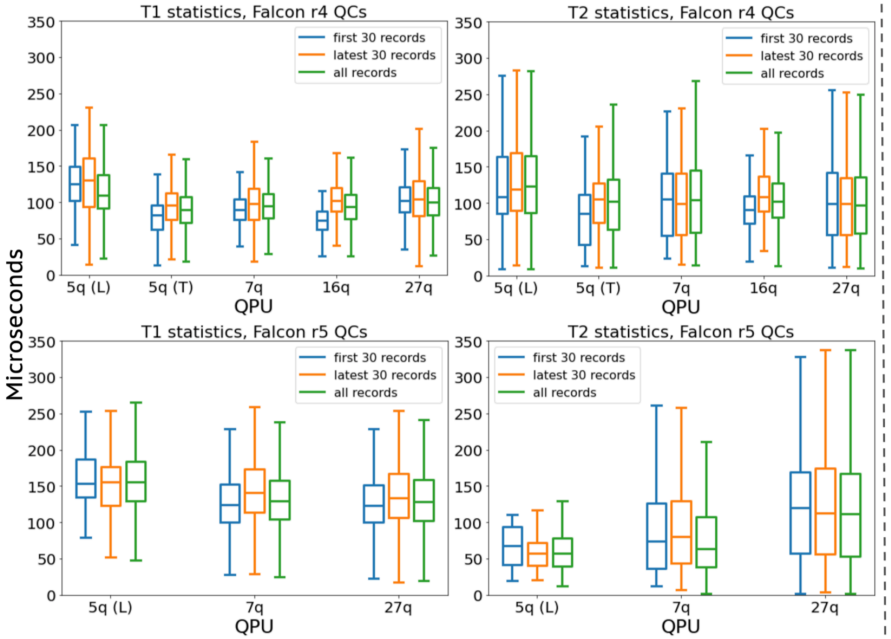
Open challenges:

- Long fingerprinting time and need for post-processing to extract the interesting features from data

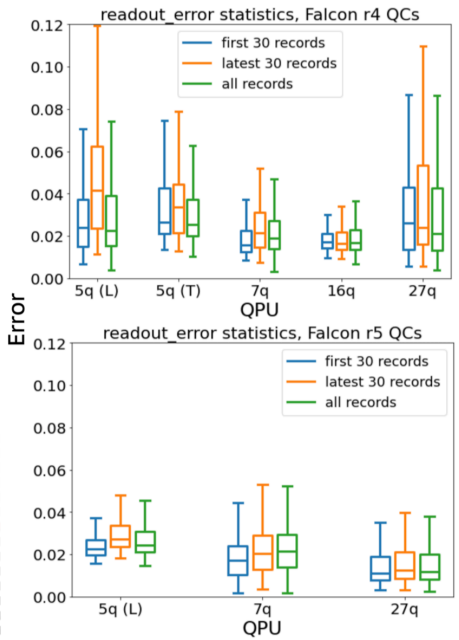
Towards Faster Fingerprinting

Is it possible to make fingerprint based on direct measurement of hardware properties, such as T1 and T2 times, readout error, gate error, frequency?

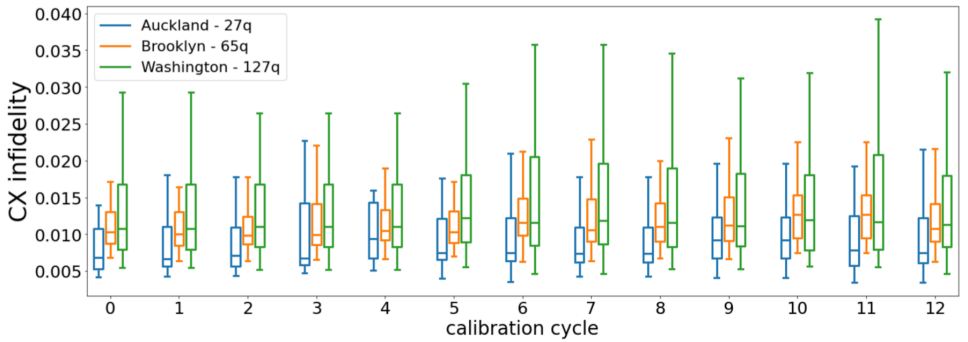
T1 and T2 Times



Readout Error



CX Gate Error

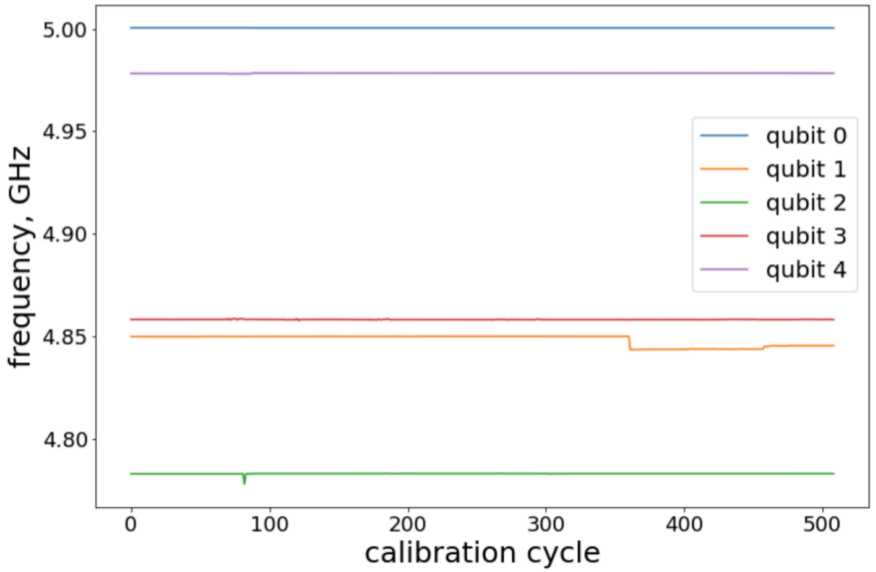


These properties are not sufficiently unique among machines for use as fingerprint

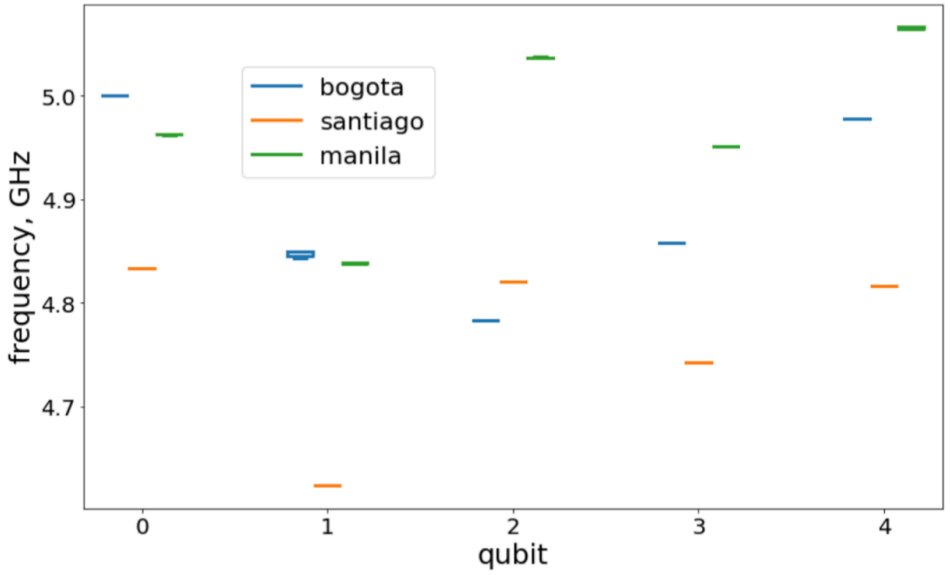
Fingerprinting Based on Unique Qubit Frequencies

Promising feature which is stable over a long time are qubit frequencies.

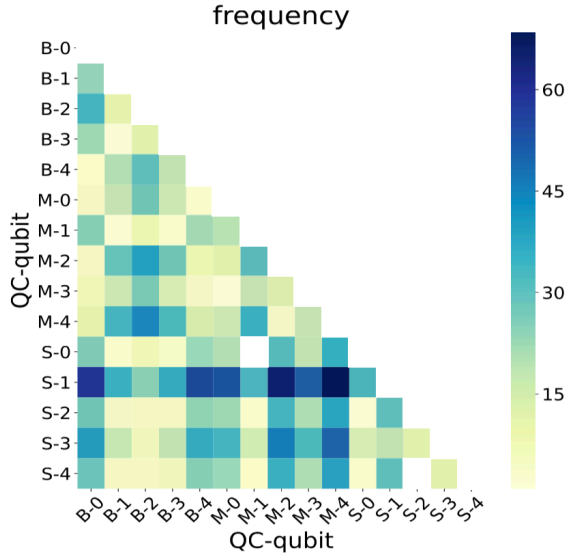
Frequency vs. calibration cycles for the five-qubit Bogota IBM QC, showing the consistency of qubit frequency over many cycles.



Comparison of frequency distribution vs. qubit for the five-qubit IBM QCs Bogota, Santiago and Manila.



Most qubits have unique and dissimilar frequencies, even across machines



Frequency Based Fingerprint

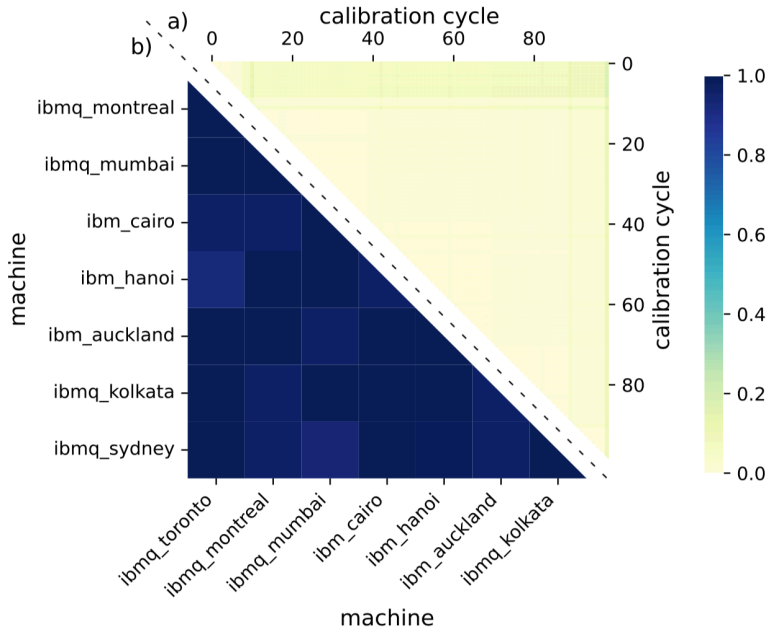
Our new fingerprint is defined as vector of qubit frequencies: $\vec{f} = \begin{bmatrix} f_0 & f_1 & \dots & f_{N-1} \end{bmatrix}^\intercal$

Similarity of the fingerprints is computed based on: $\frac{\#\text{ frequencies that differ}}{\#\text{ qubits}} = \frac{|\{k : |f_{i,k} - f_{j,k}| > \Delta_{\text{avg}}\}|}{N}$

Have good stability and uniqueness per machine:

a) Comparing similarity across many calibration cycles yields similar fingerprint

b) Comparing among machines, each tested machine gives unique fingerprint (high dissimilarity metric)



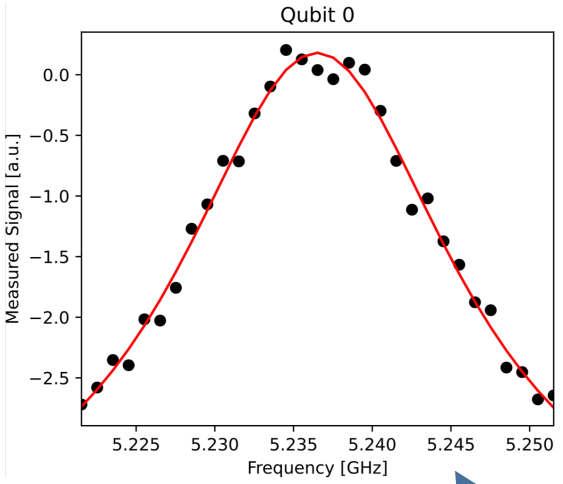
Frequency Sweep Circuit vs Calibration Data

Frequency data can be obtained from historical calibration data available from IBM

- Can evaluate effectiveness based on many months of data

Users can generate their own frequency measurements

- For pay-as-you-go IBM cloud historical data may not be available
- Quantum computer provider may hide the data on purpose
- Easily available frequency sweep circuits, 10s of seconds to run



Example frequency sweep circuit output, used to find qubit's frequency

Security implications:

- Even without historical data users can generate fingerprints and map the infrastructure

Open challenges:

- Tunable qubit architectures exist, or qubit frequency can be adjusted using laser annealing
- Need access to control frequency for frequency-sweep circuits

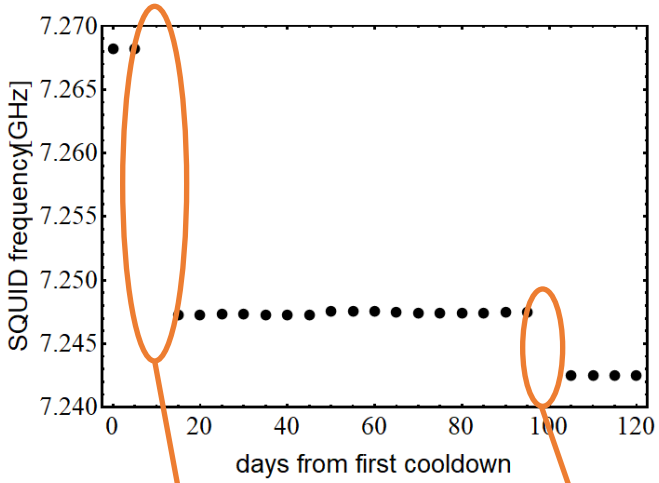
Fingerprinting Quantum Computer Infrastructure

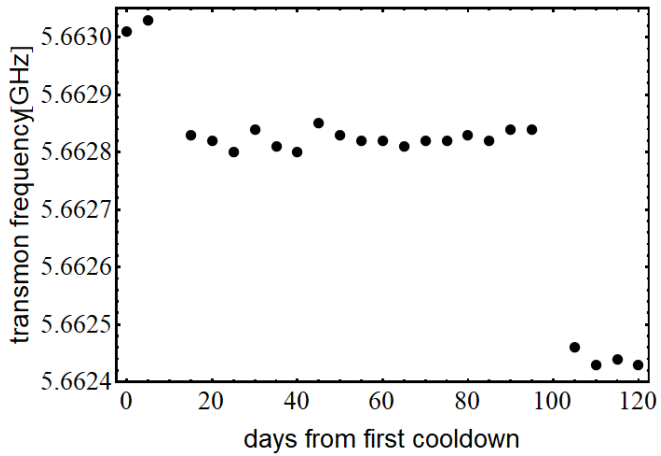
Learning About Remote Quantum Computer Infrastructure

Behavior of the quantum computers can reveal information about the infrastructure or the devices and how they are used or maintained.

Can long-term frequency changes be used to track device operation?

- Device frequency changes significantly when device is warmed up, e.g., for maintenance
- Frequency can also change due to modification of the hardware during warm up

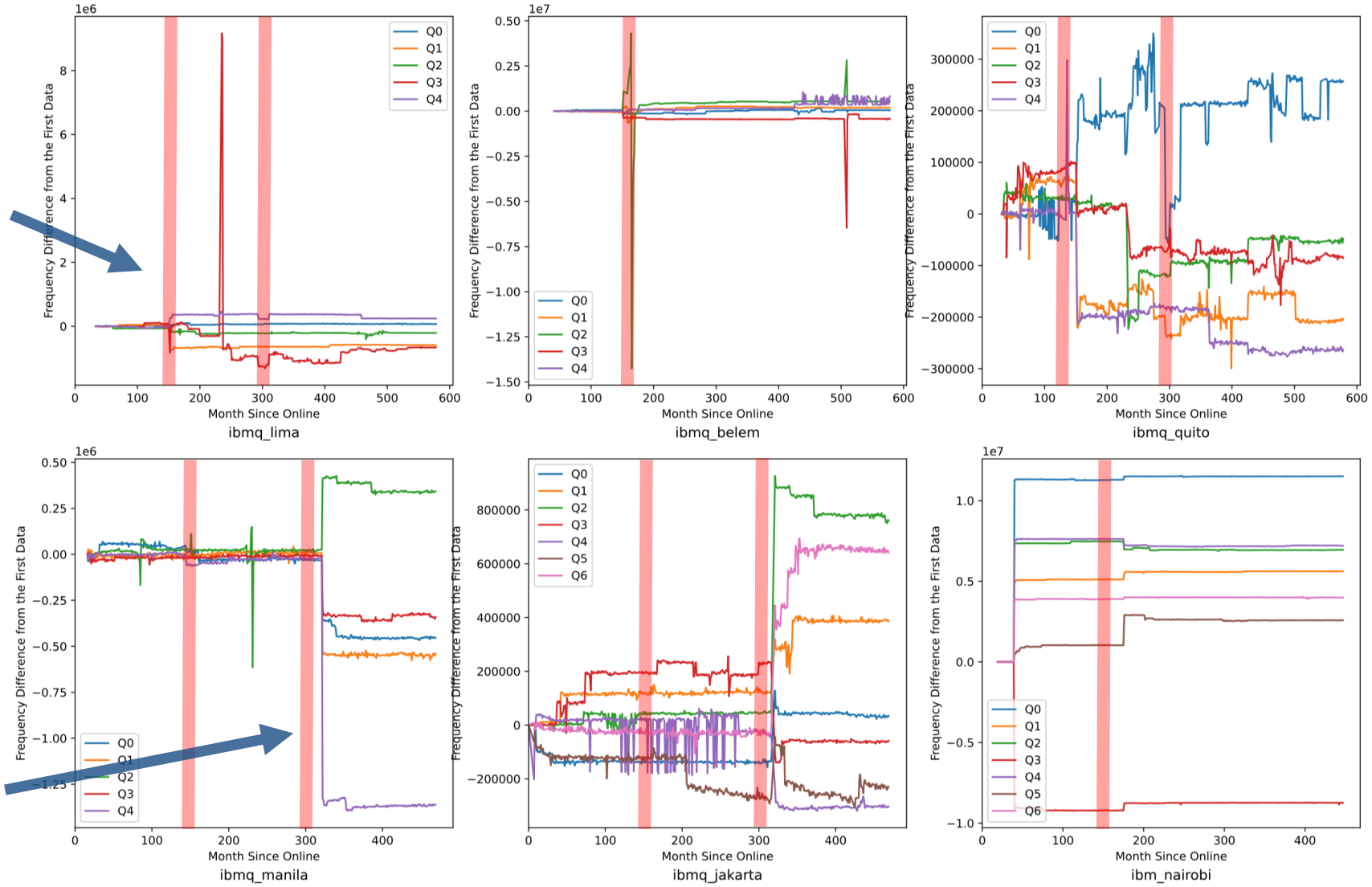




Device B	10/23/21	10/29/21-11/04/21	11/06/21	01/29/22-02/02/22	02/03/22
Freq [GHz]	7.268	warm	7.247	warm	7.242

Qubit Frequency Shifts in IBM Machines

Many devices experience frequency shift at 150 days (5 months)

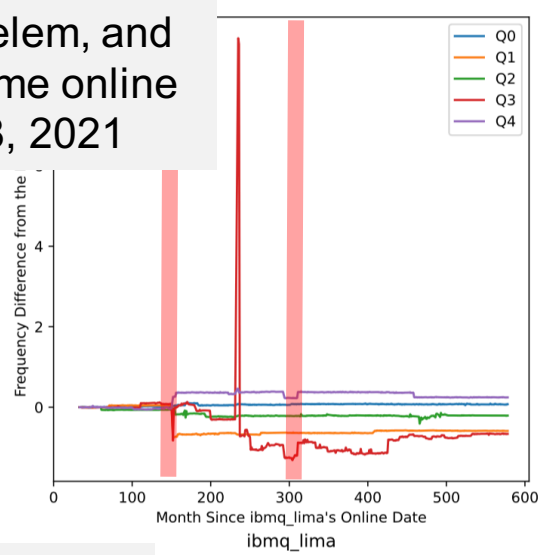


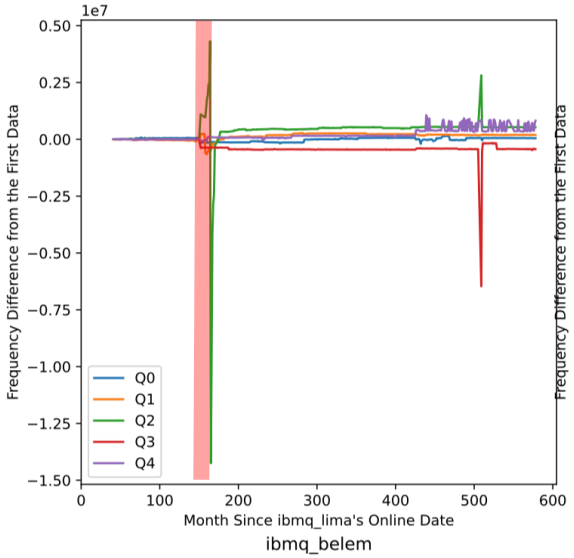
Around 300 days (10 months) there are also frequency shifts

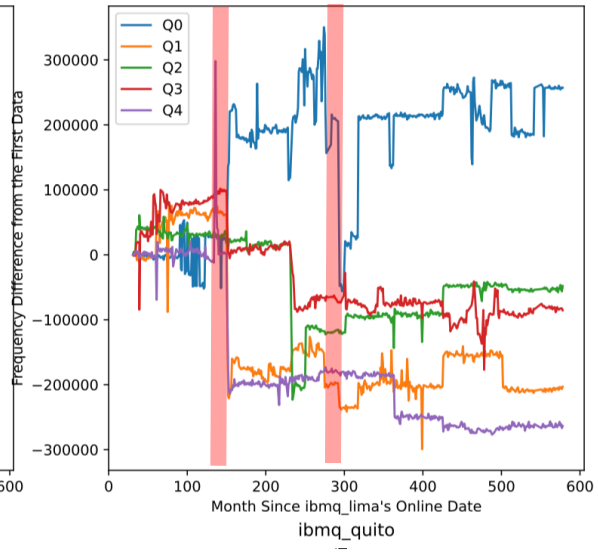
Figures show data since days online for each machine

Qubit Frequency Shifts in IBM Machines

Lima, Belem, and Quito came online Jan. 8, 2021

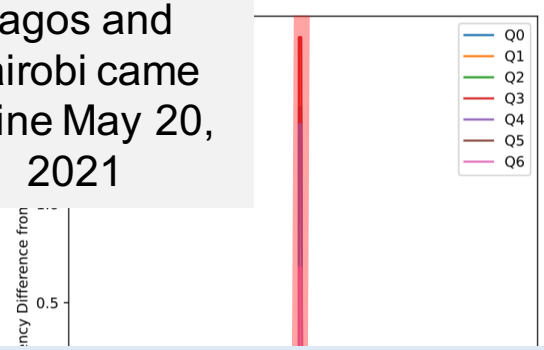


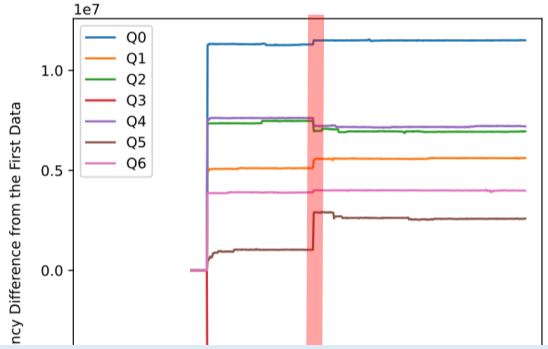




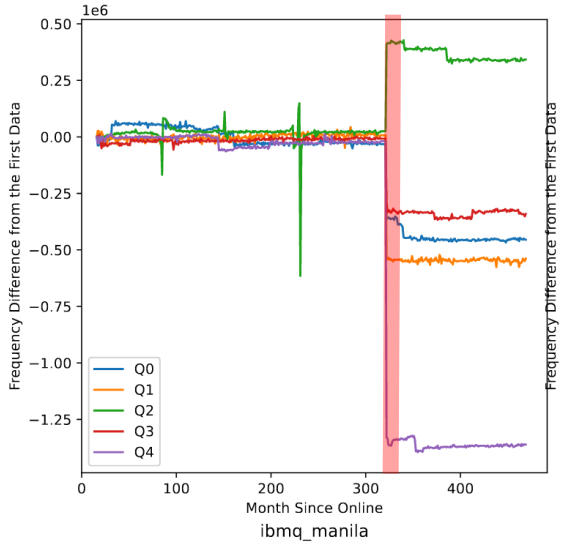
Figures show data since days when Lima was online

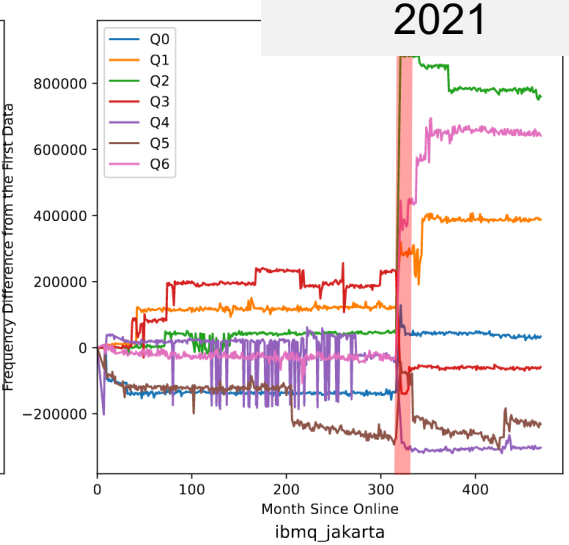
Lagos and Nairobi came online May 20, 2021





Manila and Jakarta came online April 28, 2021





Open challenges:

- Large noise in calibration data
- No reference to real physical events in IBM

Information Leaks Across Reset Gates

Reset Gate in IBM Quantum Computers

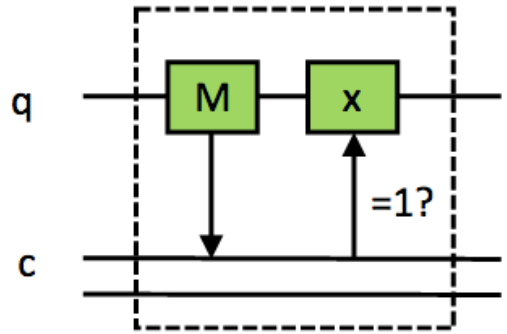
Quantum computer's qubits have to be reinitialized before any new computation starts

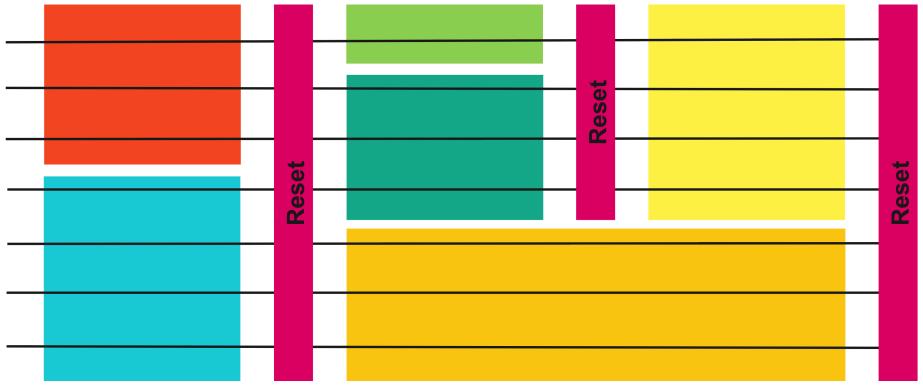
Typically perform a full system wipe to reset the qubits
- Can take up to 1000us
- Resets all qubits at same time

Reset gates exist that can reset individual qubits
- Measure qubit state
- Conditionally flips the post-measurement state from $|1\rangle$ to $|0\rangle$
- On order of 10us to execute

Benefits of reset gates
- Reset in middle of circuit
- Reset between users in single- or multi-tenant computing scenarios

Reset Gate:





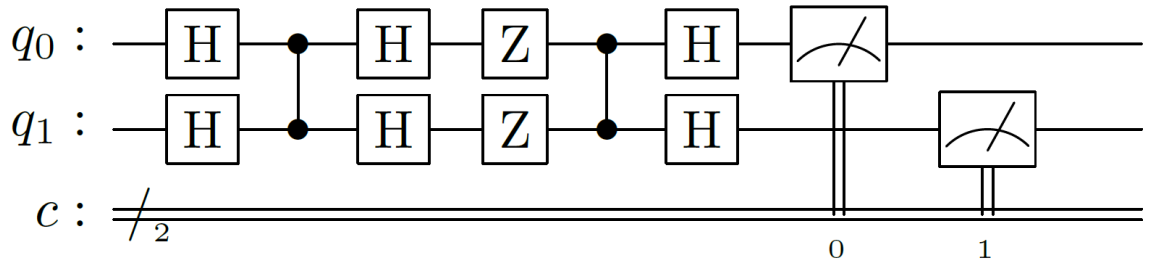
Problems if Reset Gate Does Not Work Correctly

Incorrect operation of the reset gate can create information leaks

- If attacker runs before victim, can cause incorrect initial state, possibly affecting the computation
- If attacker runs after victim, can recover some information about the final qubit state

Incorrect state at beginning can affect computation

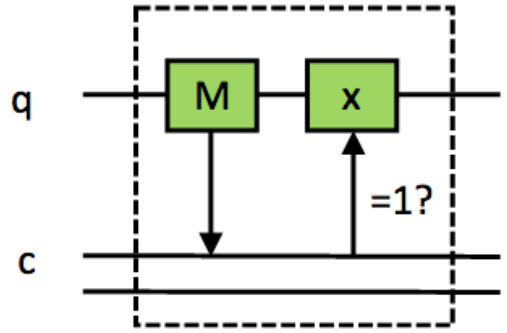
Leaky reset can allow readout of the final state of the computation

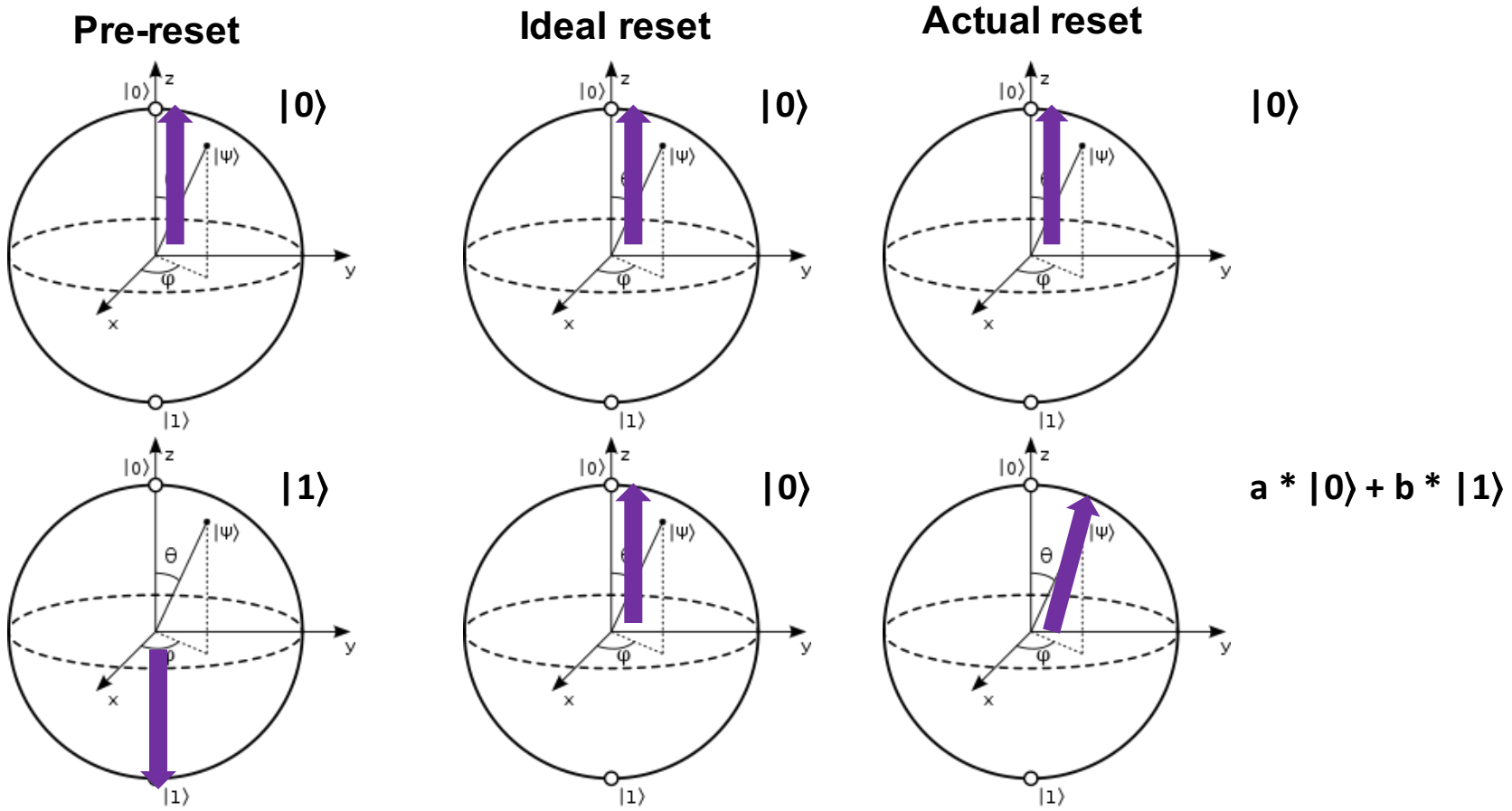


Leaky Reset Gates

We analyzed IBM superconducting qubit quantum computers

- We found that reset gate does not behave fully correctly, post-reset the state is not always $|0\rangle$

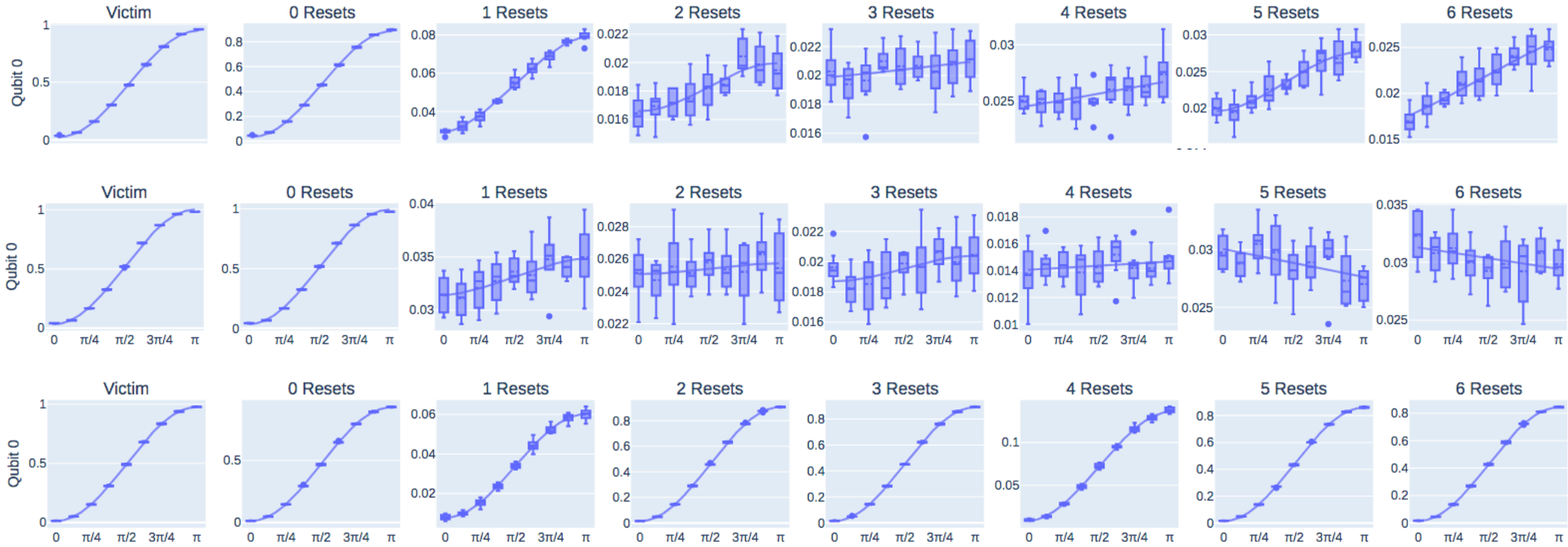




Evaluation of Leaky Reset Gates

Experimentation demonstrated that after reset, or even multiple resets, the qubit state is not exactly in the desired $|0\rangle$

- It is possible to recover the state of the qubit post reset by characterizing reset behavior of qubits
- Analyzed probability of measuring $|1\rangle$ post reset for different theta angles



Jakarta backend

Lagos backend

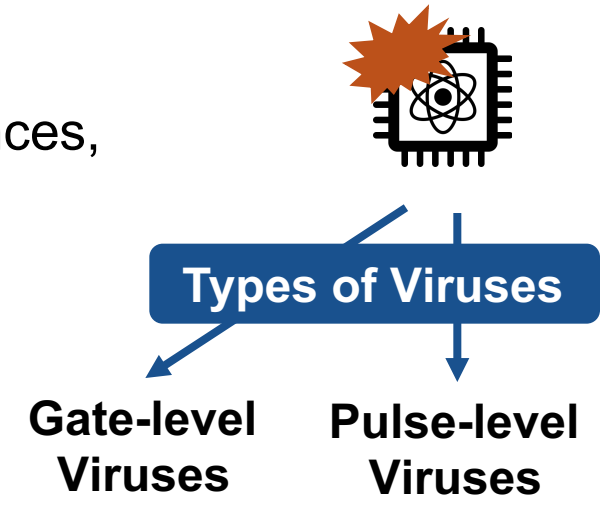
Perth backend

Towards Software Defense for Quantum Computers

Threats to Quantum Computers

We define Quantum Virus as any circuit running on a Quantum Computer used to steal information or disrupt operation of the Quantum Computer

- Gate-level viruses are built using gate-level circuits
- Pulse-level viruses are built from custom pulse sequences, need pulse-level access

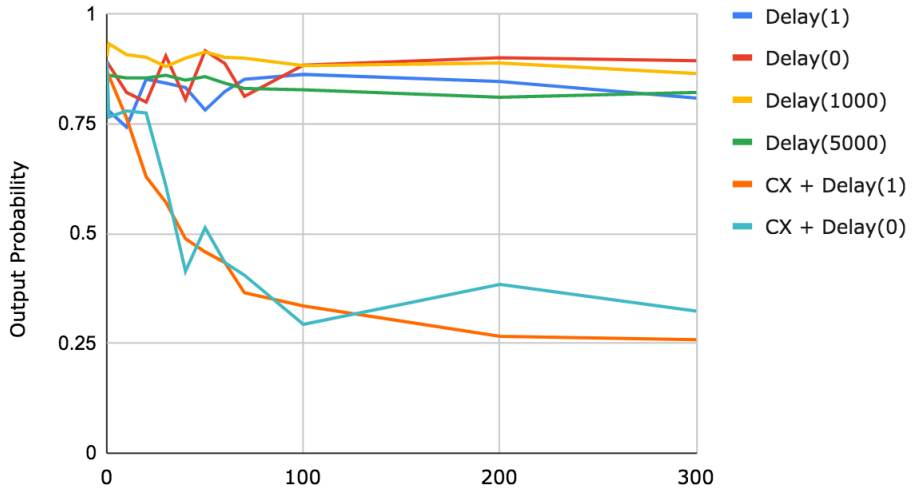


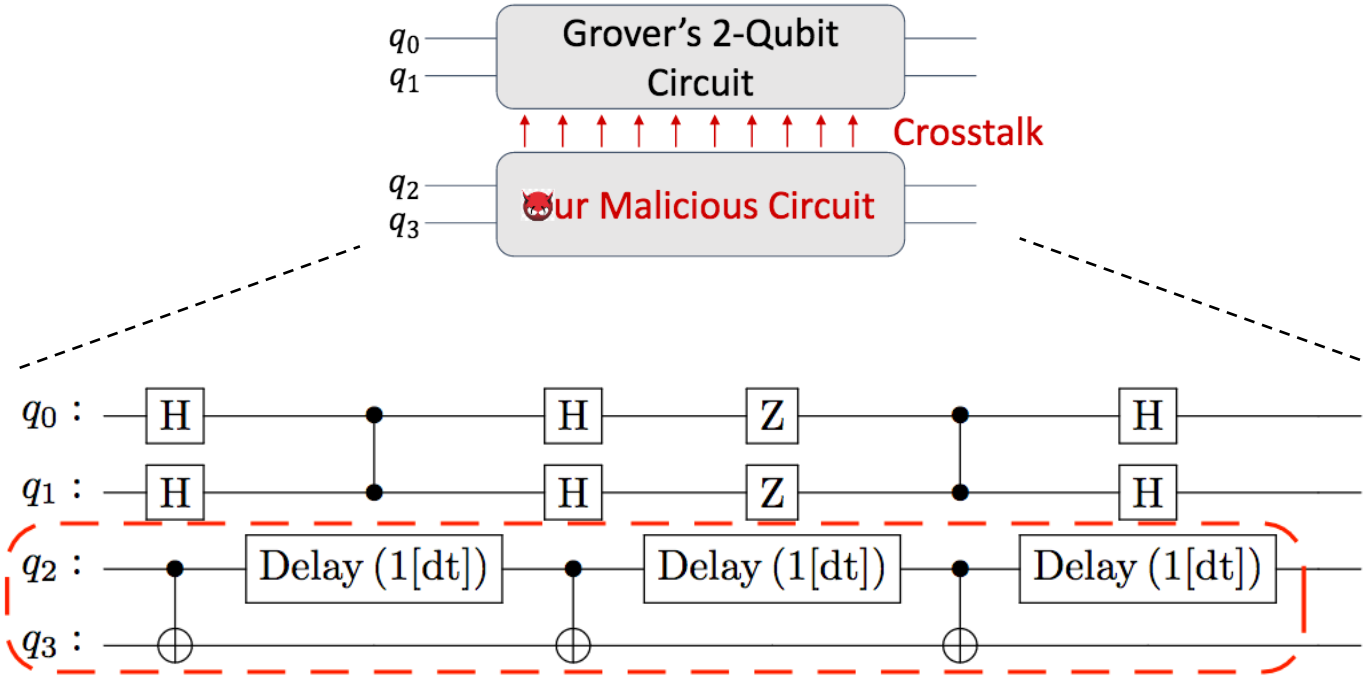
- E.g. quantum circuits are vulnerable to physical phenomenon such as **crosstalk and thus information leaks**
- E.g., today users can make any circuit they want even **power viruses and thus cause denial of service**

Quantum Computer Crosstalk Attacks

Researchers are proposing multi-tenant Quantum Computers

- But co-tenants may affect or even attack each other
- Operations on adjacent qubits induce gate errors that affect victim

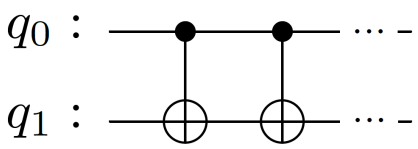




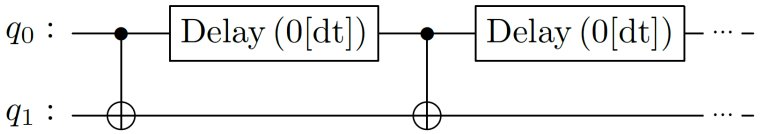
Candidate “Virus” Circuits

Different possible circuits could be designed to generate excessive crosstalk, e.g.:

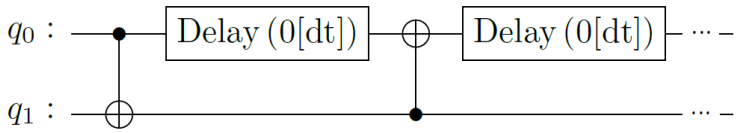
M1



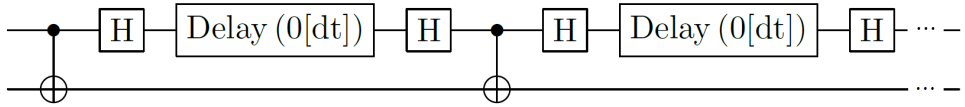
M2



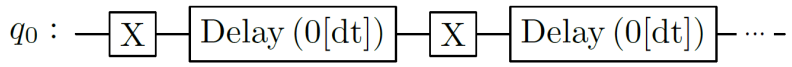
M3



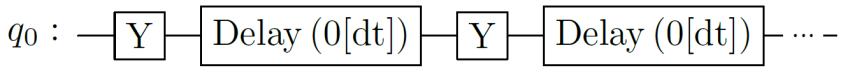
M4



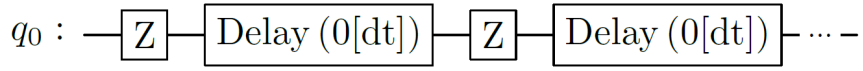
M5



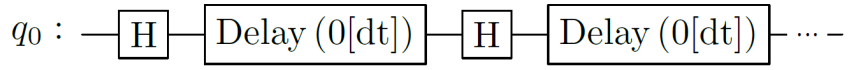
M6



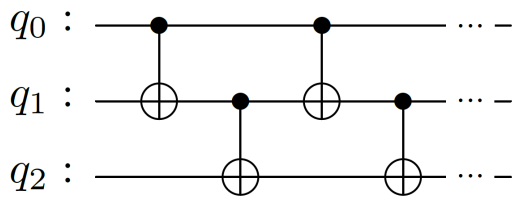
M7



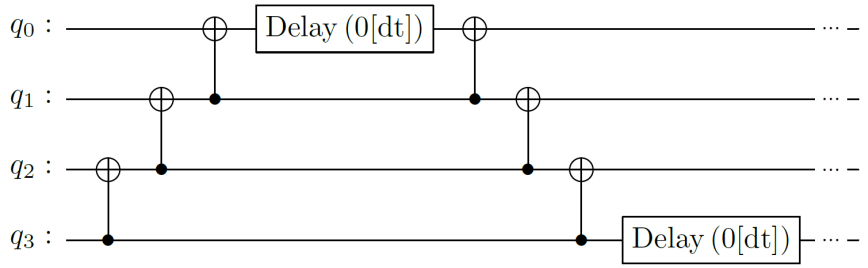
M8



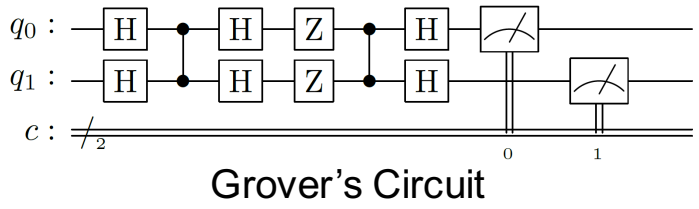
M9



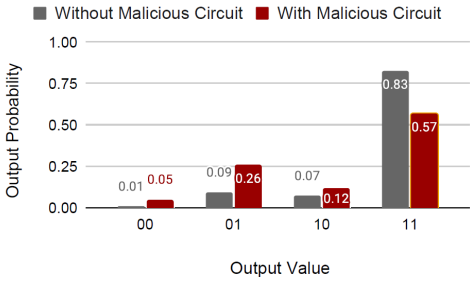
M10

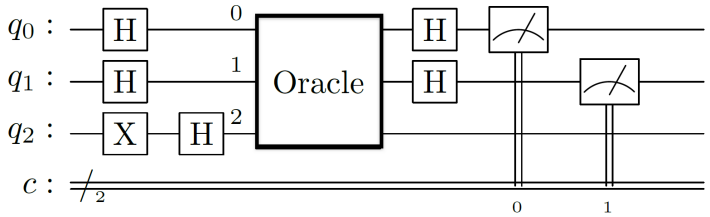


Impact of Crosstalk

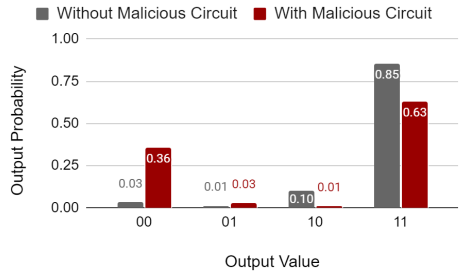


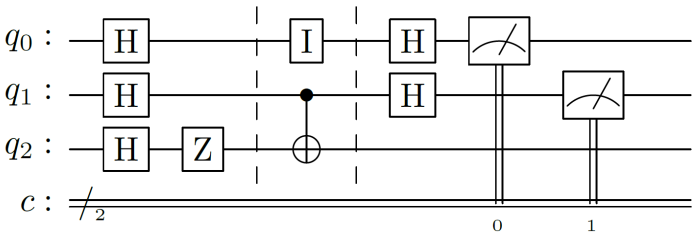
Grover's Circuit



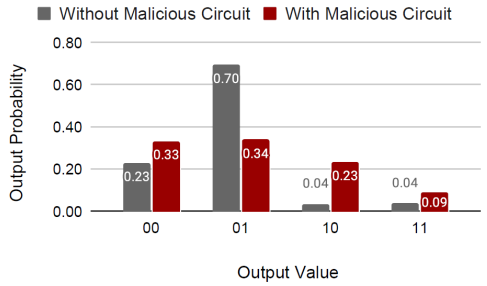


Deutsch-Josza Circuit





Bernstien-Vazirani Circuit



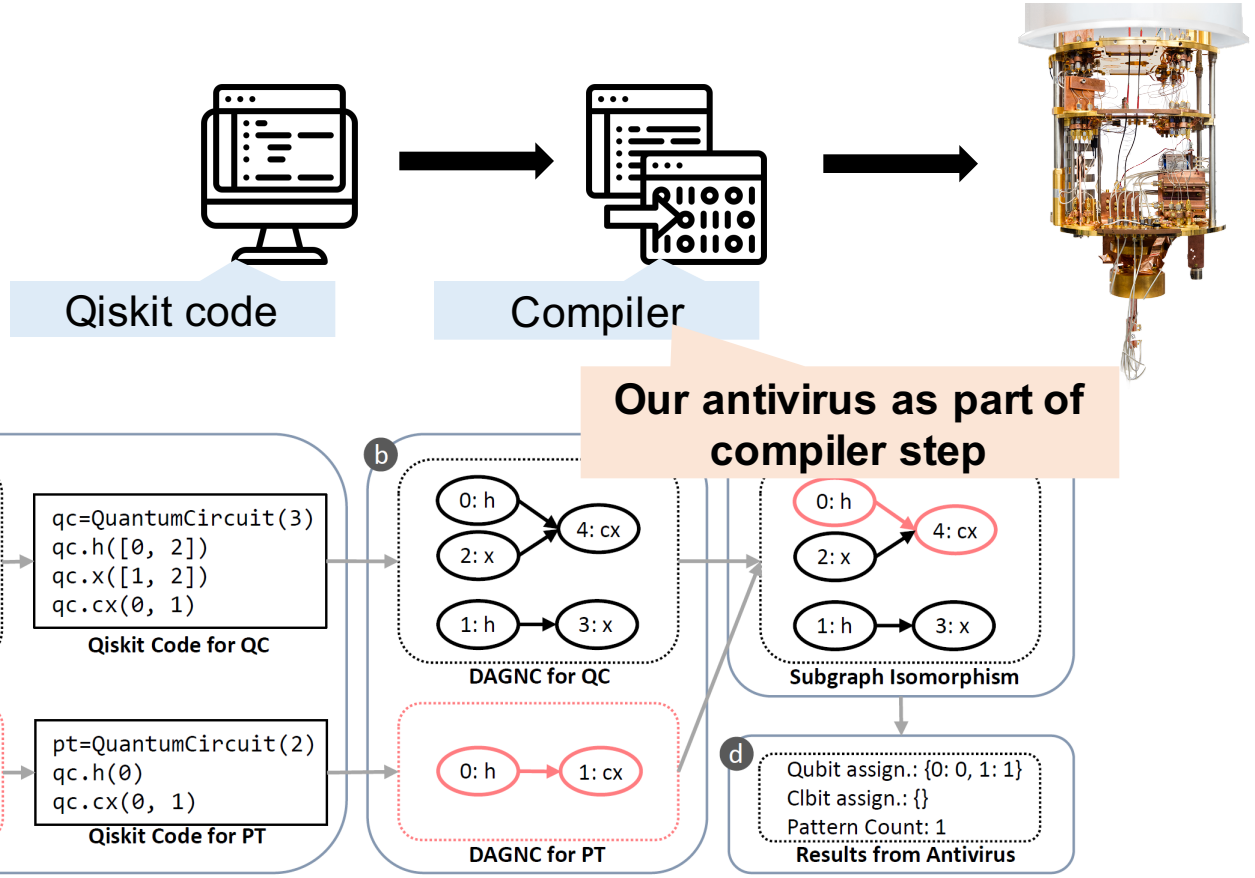
- Grover's Algorithm:
  - Provides Quadratic Speed up in Unstructured Search
- Deutsch-Jozsa Algorithm:
  - Determines whether a given Oracle is constant or balanced
- Bernstein-Vazirani Algorithm:
  - Finds out a hidden string with a single query to Oracle

Design of Quantum Computer Antivirus

We are leveraging popular Qiskit programming environment available today for Quantum Computers. Any program (including a virus) is described in Qiskit as set of quantum gates. We need to find these sets of quantum gates that correspond to a malicious circuit, i.e. a virus

Quantum gate-level viruses can be represented as graphs of the malicious quantum circuits

- Leverage subgraph isomorphism to find subgraphs representing viruses
- Run efficient algorithms on classical computer to analyze the graph representation of quantum circuit to find if it is a virus



Antivirus workflow

Difference from Classical Antivirus

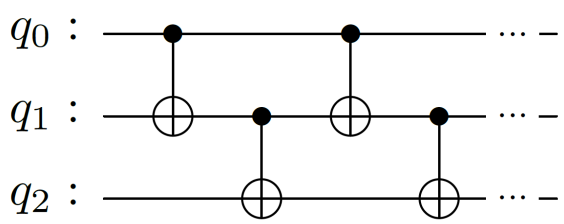
Classical Antivirus

Classical viruses are sets of instructions, need to use string pattern matching to find sequences of malicious instructions in bigger program

```
mov  al, 97
int  0x80
xchg edx, eax
push 0xAAAA02AA
mov  esi,esp
push byte 0x10
```

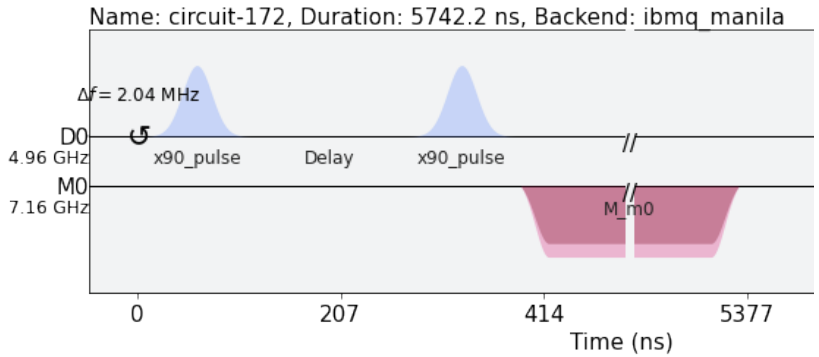
Gate-Level Antivirus

Gate-level quantum viruses are sets of quantum gates, need to use subgraph isomorphism to locate malicious circuits in bigger circuits (graph)



Pulse-Level Antivirus

Pulse-level quantum viruses use sets of control pulses, need to locate pulse patterns in larger trains of pulses



Open challenges:

- Short decoherence times make it hard to run bigger circuits and show true impact of crosstalk
- Many ways to implement same circuit

Physical Attack on Quantum Computers

Physical Attacks

Physical security attacks concern scenarios where the attacker has physical access to the target device

- Physical access if device is small or easy to capture, e.g., stolen smartphone, laptop left in hotel room, etc.
- Physical access of untrusted employee in data center or physical access of government or other agency

Physical attacks pros and cons:

- Much more powerful than remote or software attacks
- But also usually of concern when dealing with very sensitive business data or intellectual property, government data, or data that could impact safety of dissidents

Example, a **fault injection attack** is a physical attack on the device to inject the fault in the system deliberately to change its intended behavior.

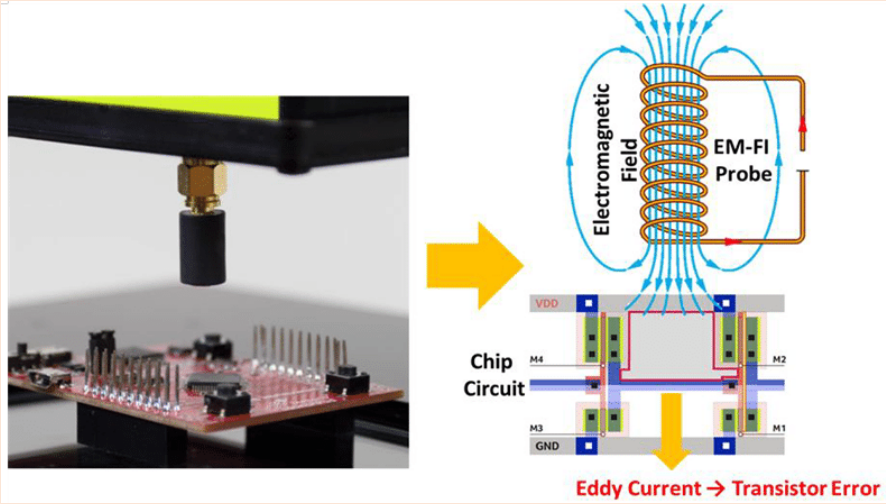


Image: Lim, et al. "Novel fault injection attack without artificial trigger." Applied Sciences 10.11 (2020): 3849.

Physical Attacks on Quantum Computers

Example components of a quantum computing system, based on a public image of a quantum computer setup.

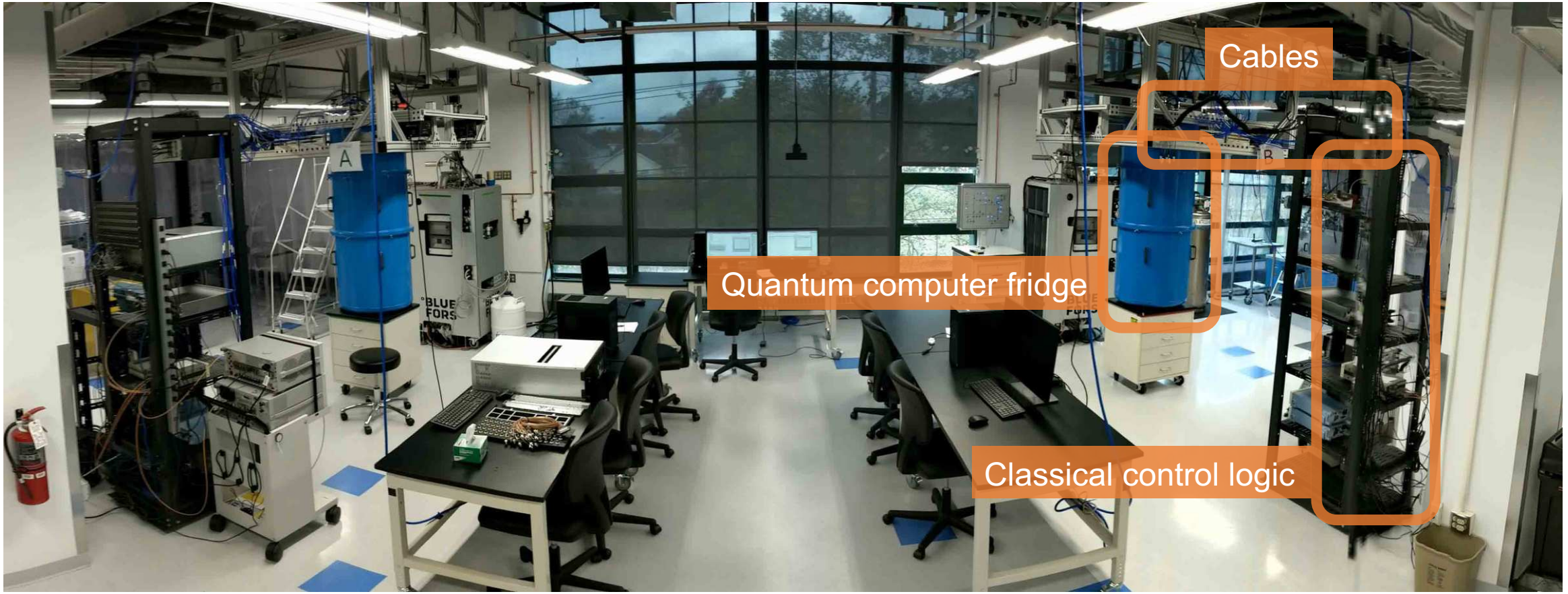
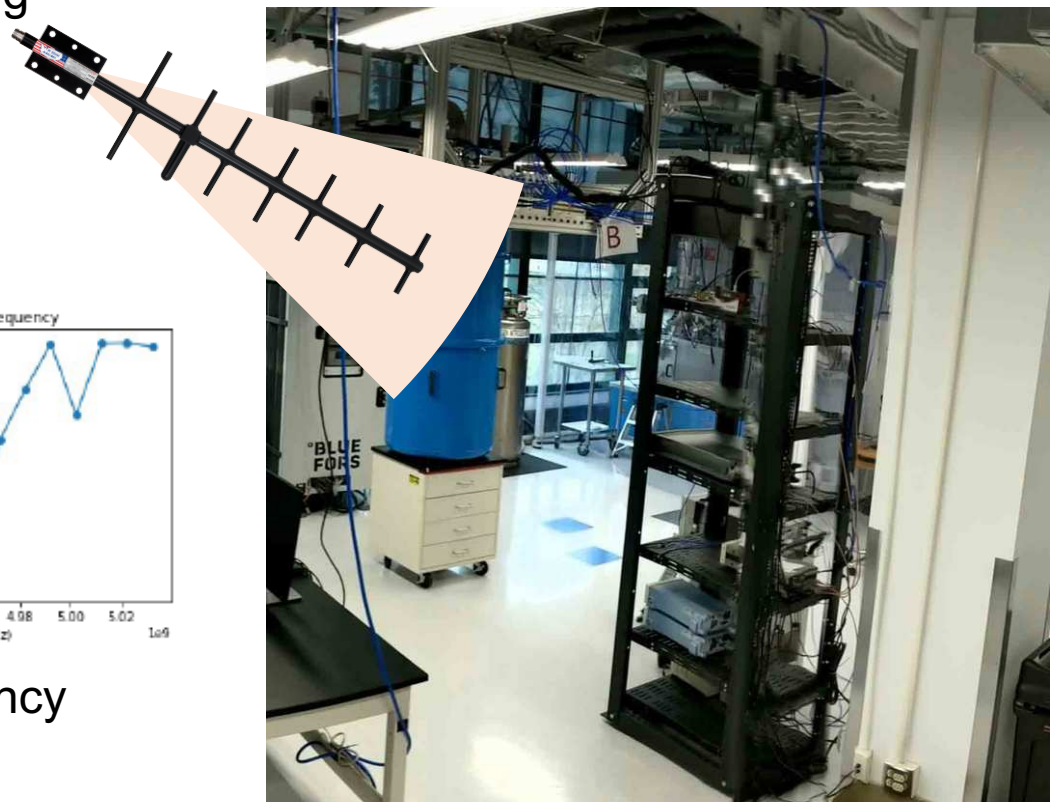


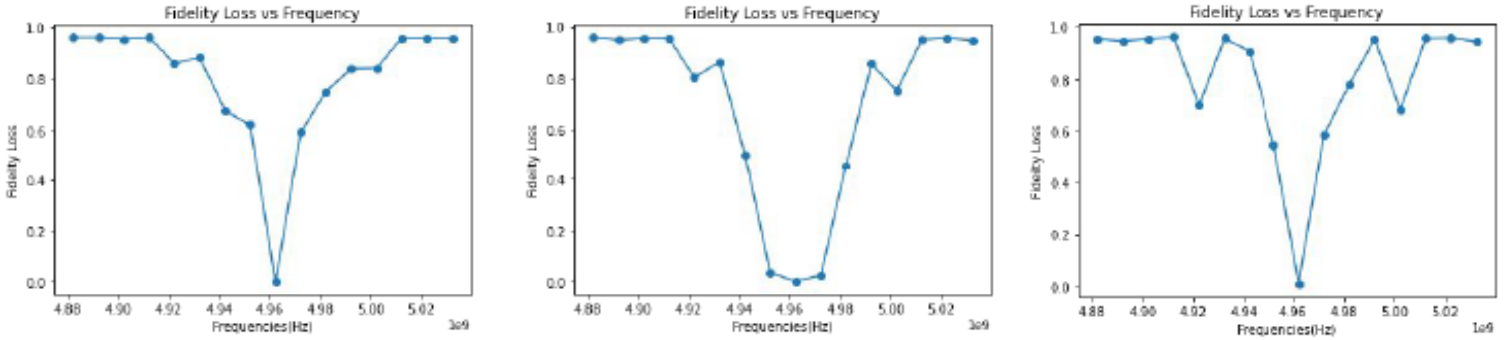
Image: https://quantumcircuits.com/about

Possible Active Attacks

Active attacker can use external EM source to try to inject signals or modify signals controlling quantum computers to cause wrong computation or later qubit state



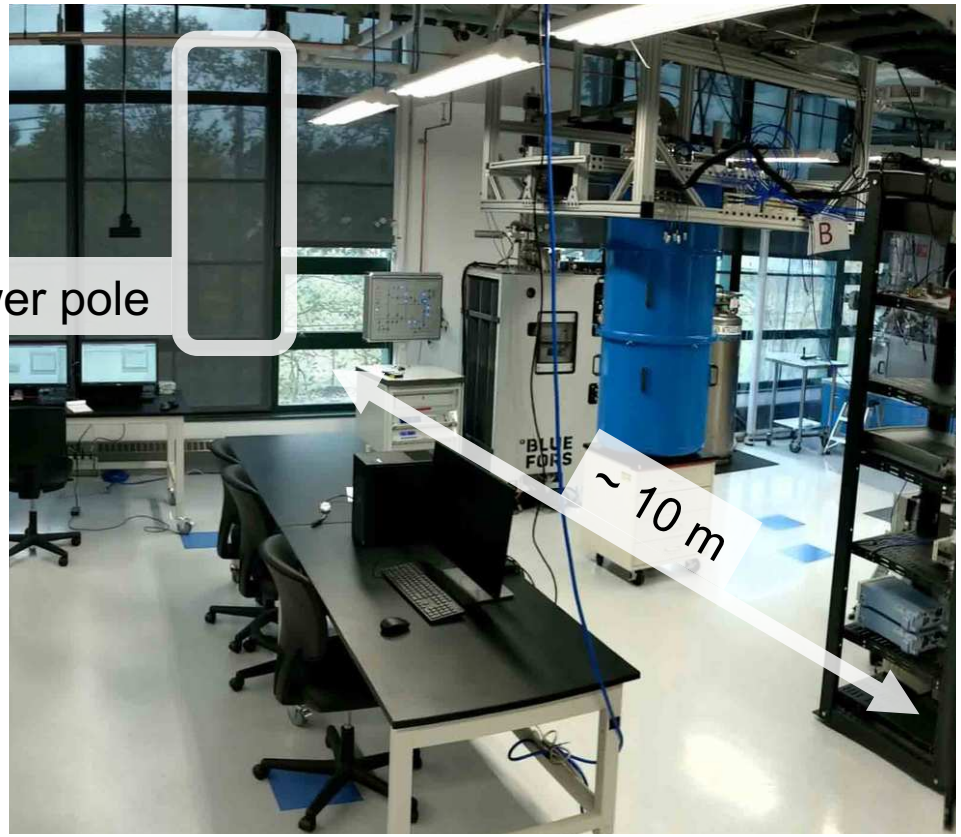
Simulation of perturbation of RF pulse frequency
of pulses used to control sequence of 5, 7, and 9 X gates:

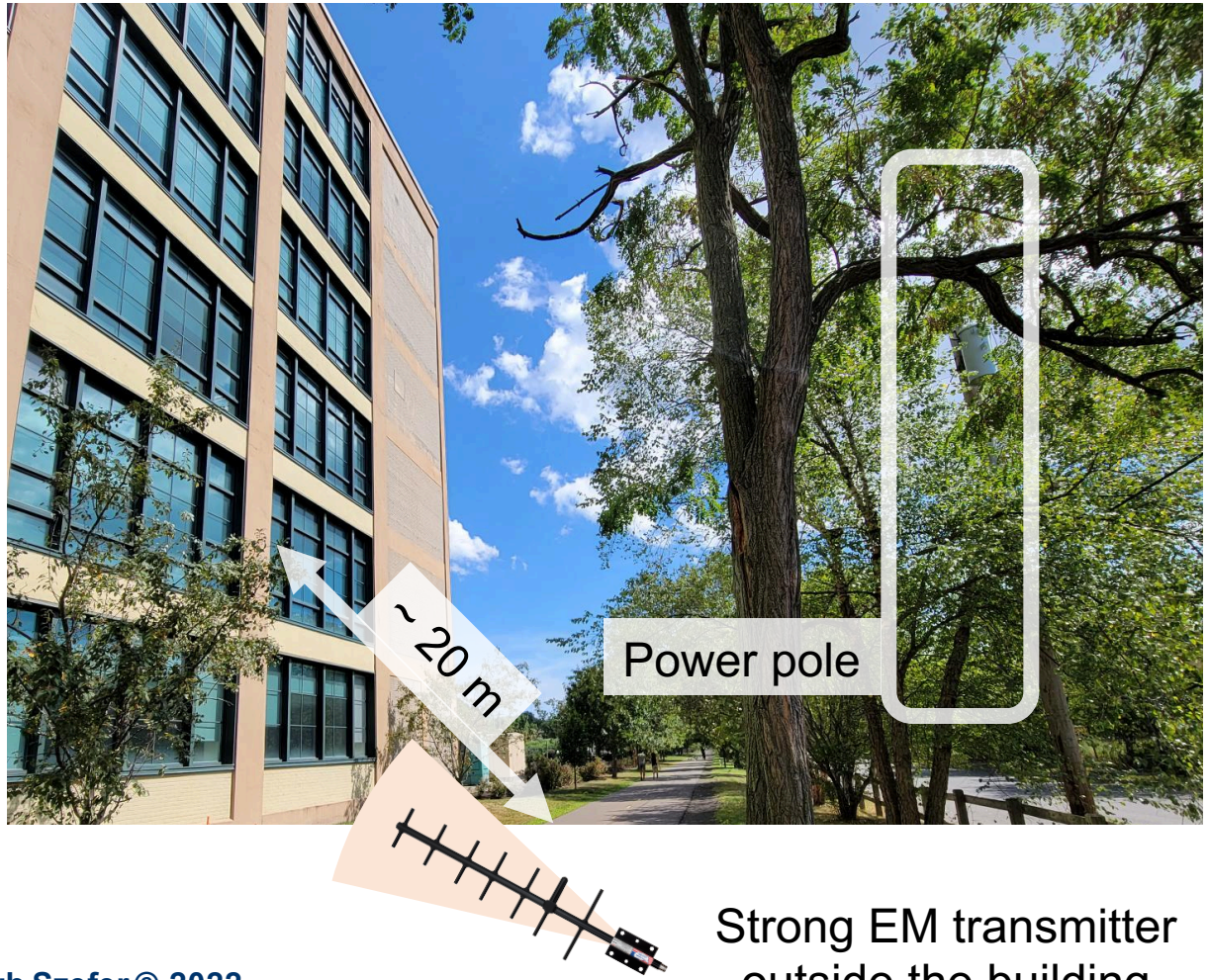


- Shifting frequency by 15Mhz to 30Mhz from proper frequency already significantly cuts down on fidelity of the X gate
- With bigger frequency shift, can you effectively disable X gate, leading to incorrect computation results?

Possible Active Attacks

Location of the quantum computing system can make it vulnerable to physical attacks.





Possible Passive Attack

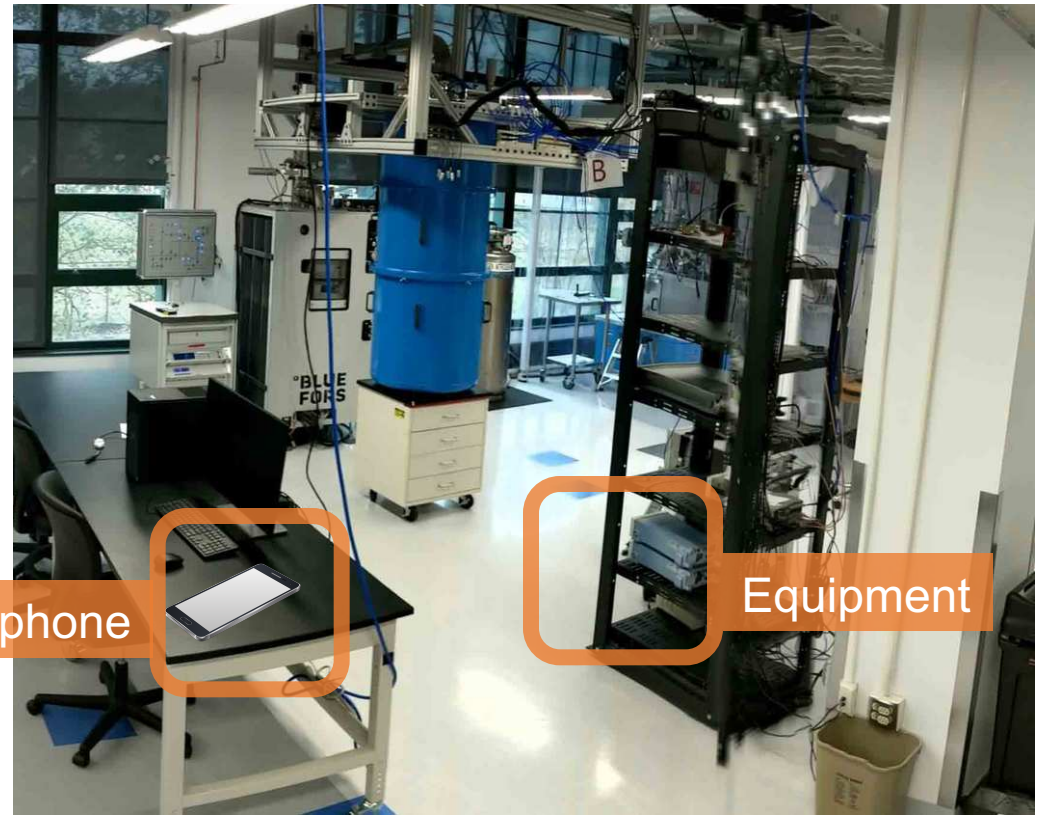
It is well known from classical computers are passive attacks where attacker “listens in” on the victim to learn about program execution or operations of the computer

Modern smartphones have many sensors

- Accelerometer, compass, gyroscope, etc.
- WiFi, cellular network, AM/FM receivers, etc.

Is it possible to capture controller equipment or other emanations to obtain or reverse-engine:

- Approximate, or even full, quantum circuit that was executed?
- Type of qubits or other technologies used?



Open challenges:

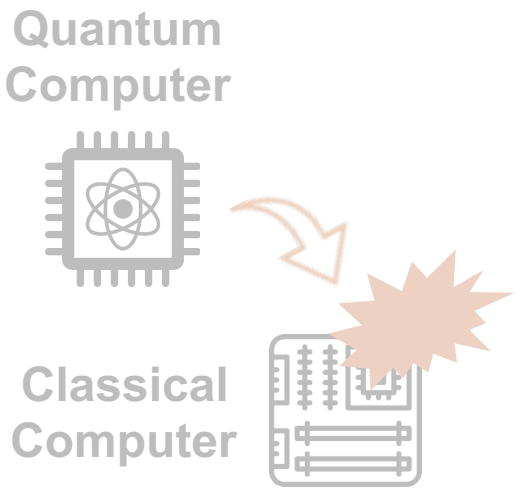
- Access to quantum computers and testing the attacks

Wrap Up

Exploring New Side of Quantum Computer Security

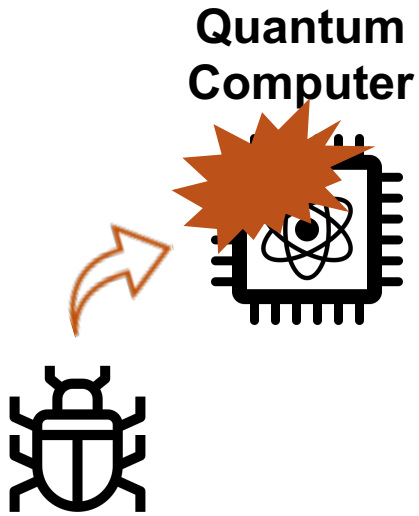
Others

Almost all of existing quantum computer security research focuses on attacks using the computers to break classical cryptography



Us

Our research focuses on protecting quantum computers from security attacks to protect the algorithms and data on quantum computers



Talk Review

- Fingerprinting Quantum Computers
- Fingerprinting Quantum Computer Infrastructures
- Information Leaks Across Reset Gates
- Toward Software Defense of Quantum Computers
- Physical Attacks on Quantum Computers

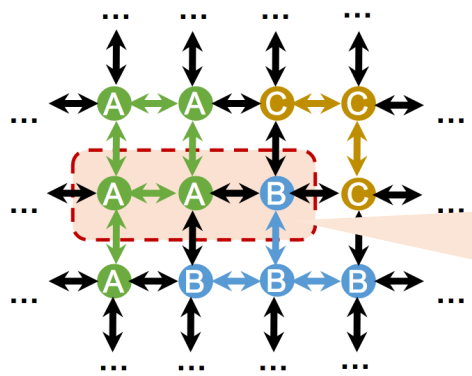
Potential Losses If There Is No Quantum Computer Security

Quantum Computers can Generate Results not Possible on Classical Computers

- Just as classical computers are vulnerable to security attacks and viruses, so are quantum computers. The data and intellectual property generated on quantum computers will be something unique

Many Potential Losses to Data or Business

- **Manipulation or Leakage of data** – malicious viruses (circuits) can use crosstalk to cause victim circuit to generate wrong data; or leak results of computation
- **Reverse engineering quantum computers** – malicious viruses (circuits) could try to perform computations that have no purpose other than discovering how the underlying hardware works, thus leaking secrets about the IP of the hardware
- **Loss of reputation** – any security attack will also result in loss of reputation and income for a company, and conversely



E.g. malicious circuit (qubits A) can affect parts of victim circuit (qubits B) via crosstalk (crosstalk region in red)

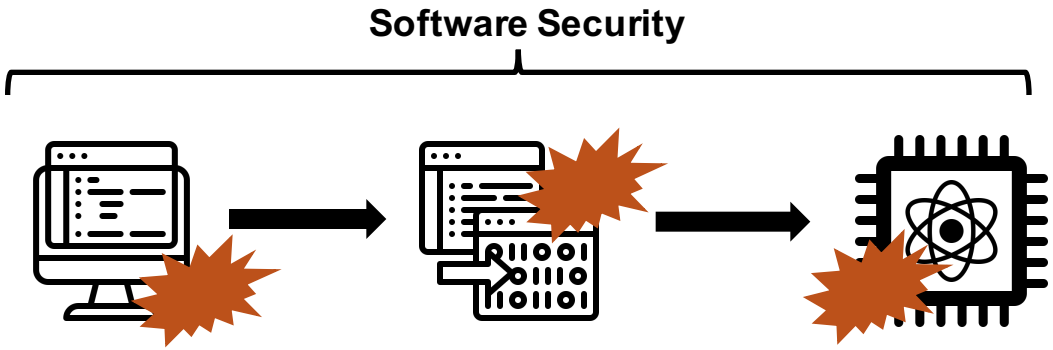
Potential for Defining Quantum Computer Cybersecurity

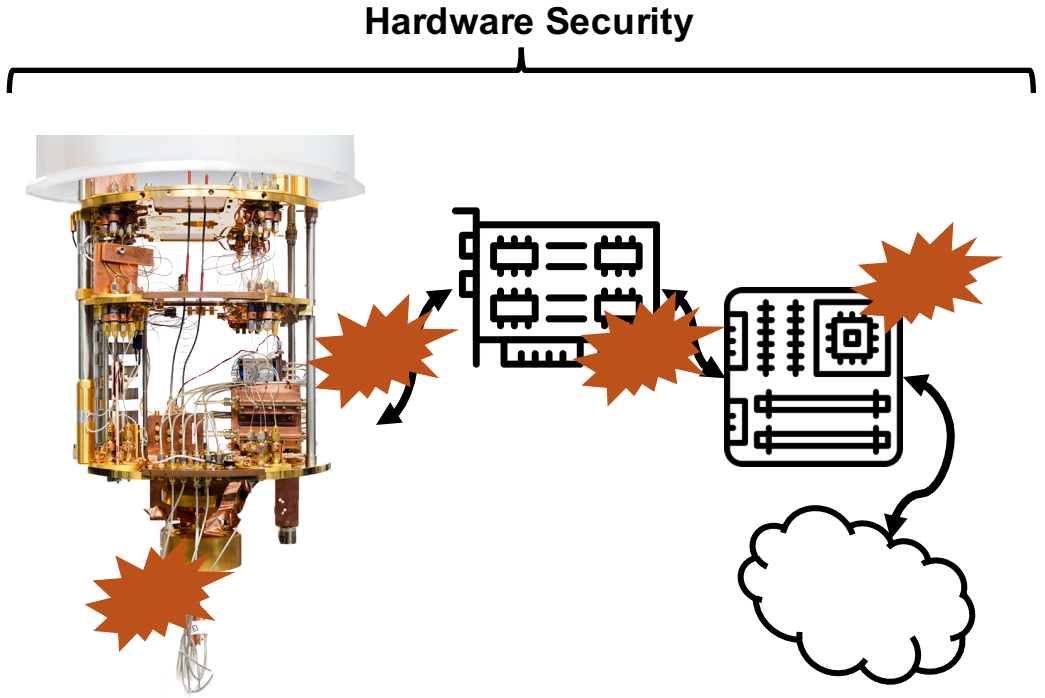
Many ideas from classical computer hardware security can be applied to quantum computers

- Directly apply prior ideas to classical components of the quantum computers
- Translate high-level ideas of information leaks, viruses, denial-of-service, etc., to quantum computers

Challenges and potential at Yale

- Access to and testing with the computers is a limiting factor for many security researchers
- Mindset of “too early” to think about security of the machines





Acknowledgements

Prof. Yongshan Ding

Dr. Yao Lu

Dr. Kaitlyn Smith (U. Chicago)

Prof. Swamit Tamu (Wisc.)

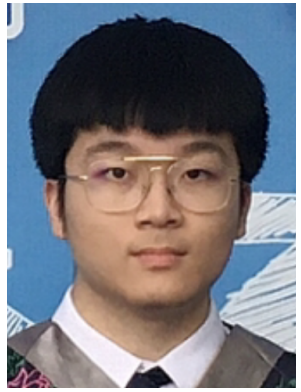
Shuwen Deng

Allen Mi

Sanjay Deshpande

Ferhat Erata

Theodoros Trochatos



Chuanqi Xu

Thank You!