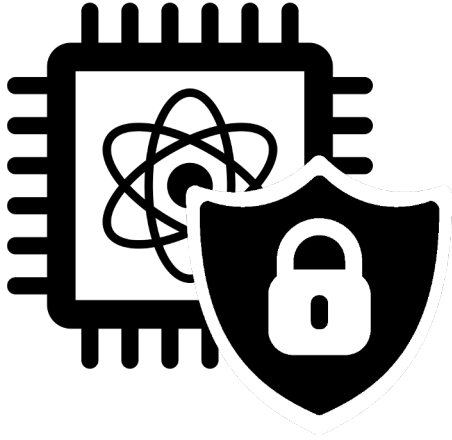




Tutorial on Security of Quantum Computing Systems

QCE Tutorial

Sept. 17, 2026

Prof. Jakub Szefer (jakub.szefer@northwestern.edu)

Electrical and Computer Engineering

Northwestern University



Computer Architecture
and Security Lab (CASLAB)



Northwestern
University

Tutorial Outline

- 1:00pm – 1:30pm: Introduction and Motivation
 - What is Quantum Computing and Security?
 - Brief History of Quantum Computing and Motivation for Security Research
 - Introduction to Quantum Computation and Security Threats
- 1:30pm – 2:30pm: Crosstalk and Fault Injection in NISQ Quantum Computers
 - Crosstalk and Fault Injection Among Qubits
 - Fault Injection in Reset Gates
- 2:30pm – 3:00pm: Coffee Break
- 3:00pm – 3:45pm: Side Channels in NISQ and FTQC Quantum Computers
- 3:45pm to 4:30pm: Trusted Execution Environments for Quantum Computers
- 4:00pm: End



Resource: Quantum Security Tutorials Web Page

CASLAB Home Our Group Publications Books Tutorials

Next Tutorial in:
no upcoming tutorial is currently scheduled

Next:

[Tutorial on Security of Quantum Computing Systems](#)

September 17, 2026, co-located with QCE 2026.

Future:

Winter School on Attacks, Defenses, and Secure Design of Quantum Computing Systems

November 11, 2026, co-located with QCCS 2026.

Past:

Tutorial on Quantum Computer Architecture Security

June 27, 2026, co-located with ISCA 2026.

Tutorial on Security of Quantum Computing Systems

August 31, 2025, co-located with QCE 2025.

Tutorial on Quantum Computer Architecture Security

June 21, 2025, co-located with ISCA 2025.

© 2026 Jakub Szefer

Tutorials on Classical and Quantum Computer Architecture and Hardware Security

About: A series of tutorials on classical and quantum computer architecture and hardware security, presented by Prof. Jakub Szefer of the Computer Architecture and Security Lab (CASLAB) at Northwestern University.

Tutorials on Classical and Quantum Computer Architecture and Hardware Security

Prof. Jakub Szefer (jakub.szefer@northwestern.edu)
Electrical and Computer Engineering
Northwestern University

Computer Architecture and Security Lab (CASLAB) Northwestern University



Prior tutorials include: ISCA 2026, ISCA 2025, HOST 2025, ICCAD 2024, QCE 2023, HOST 2021, 2019, ACACES 2019, HOST 2019, HiPEAC 2019, and HOST 2018.



Computer Architecture
and Security Lab (CASLAB)



Northwestern
University

Resource: Quantum Computer Hardware Cybersecurity BibTeX

 **qc-hardware-cybersecurity-bibtex** Public

 Pin  Unwatch **4**  Fork **7**  Star **15**

 main  1 Branch  0 Tags  Add file  Code

 **caslab-code** Updating research paper list with recent and older papers, mainly 202... 14a4309 · now 34 Commits

 README.md	Updating email address in README file.	last year
 refs-qc-hardware-cybersecurity-papers.bib	Updating research paper list with recent and older papers,...	now
 refs-qc-hardware-cybersecurity-surveys.bib	Update refs-qc-hardware-cybersecurity-surveys.bib	11 months ago

 **README**

About

This repository contains a BibTeX bibliography file with references to research papers pertaining to security of quantum computers. Anybody is encouraged to contact the author or make pull request to add papers they would like to be considered for inclusion in the bibliography. Papers on certain topics such as post-quantum cryptography or quantum key distribution are excluded from this bibliography so that the focus can remain only on research papers dealing with attacking and defending quantum computer systems, architectures, and hardware.

Contact

To have papers considered for addition to this list, please create a pull request or or e-mail the author at: jakub.szefer@northwestern.edu

About

List of references for quantum computer hardware cybersecurity papers.

-  Readme
-  Activity
-  **15 stars**
-  **4 watching**
-  **7 forks**

Releases

No releases published
[Create a new release](#)

Packages

No packages published
[Publish your first pack](#)

Contributors

4

-  caslab-code
-  cnpapado Kc
-  chuanqixu C
-  yizhuo1007



Resource: YouTube Lectures

**Secure Quantum Computing**

Prof. Jakub Szefer
Electrical and Computer Engineering
Northwestern University

Class Session 8
Topic: Quantum Computing Basics, Part 2

Secure Quantum Computing / CE 395 / ...

by Jakub Szefer

Playlist • 11 videos • 250 views

This playlist contains video recordings of lectures from the Secure Quantum Computing course at Northwestern University. [more](#)

▶ Play all

🔖

🔗

⋮

**Secure Quantum Computing**

Prof. Jakub Szefer
Electrical and Computer Engineering
Northwestern University

Class Session 8
Topic: Quantum Computing Basics, Part 2
1:07:23

Secure Quantum Computing / Spring 2026 / Class 8 / Quantum Computing Basics, Part 2

Jakub Szefer

18 views • 2 weeks ago

⋮

**Secure Quantum Computing**

Prof. Jakub Szefer
Electrical and Computer Engineering
Northwestern University

Class Session 7
Topic: Quantum Computing Basics, Part 1
53:19

Secure Quantum Computing / Spring 2026 / Class 7 / Quantum Computing Basics, Part 1

Jakub Szefer

43 views • 3 weeks ago

⋮

**Secure Quantum Computing**

Prof. Jakub Szefer
Electrical and Computer Engineering
Northwestern University

Class Session 6
Topic: Threat Categories for Quantum Computing, Part 2
59:45

Secure Quantum Computing / Spring 2026 / Class 6 / Threat Categories for Quantum Comp. Sys., Part 2

Jakub Szefer

173 views • 1 month ago

⋮

**Secure Quantum Computing**

Prof. Jakub Szefer
Electrical and Computer Engineering
Northwestern University

Class Session 4
Topic: Threat Categories for Quantum Computing, Part 1
54:28

Secure Quantum Computing / Spring 2026 / Class 4 / Threat Categories for Quantum Comp. Sys., Part 1

Jakub Szefer

90 views • 1 month ago

⋮

**Secure Quantum Computing**

Prof. Jakub Szefer
Electrical and Computer Engineering
Northwestern University

Class Session 3
Topic: Computer Security Basics, Part 2
1:00:04

Secure Quantum Computing / Spring 2026 / Class 3 / Computer Security Basics, Part 2

Jakub Szefer

134 views • 1 month ago

⋮

**Secure Quantum Computing**

Prof. Jakub Szefer
Electrical and Computer Engineering
Northwestern University

Class Session 2
Topic: Computer Security Basics, Part 1
1:12:52

Secure Quantum Computing / Spring 2026 / Class 2 / Computer Security Basics, Part 1

Jakub Szefer

268 views • 1 month ago

⋮

**Secure Quantum Computing**

Prof. Jakub Szefer
Electrical and Computer Engineering
Northwestern University

Class Session 1
Topic: Introduction to Secure Quantum Computing Course
1:14:13

Secure Quantum Computing / Spring 2026 / Class 1 / Introduction to Secure Quantum Computing Course

Jakub Szefer

371 views • 1 month ago



Resource: Upcoming QCCS Symposium 2026

[QCCS 2026](#) [Program](#) [Venue](#) [Directions](#) [Contact](#) [Prior QCCS 2025](#) [Prior QCCS 2024](#) [Prior QCCS 2023](#)

QCCS 2026 **4th Annual Quantum** **Computer Cybersecurity** **Symposium**

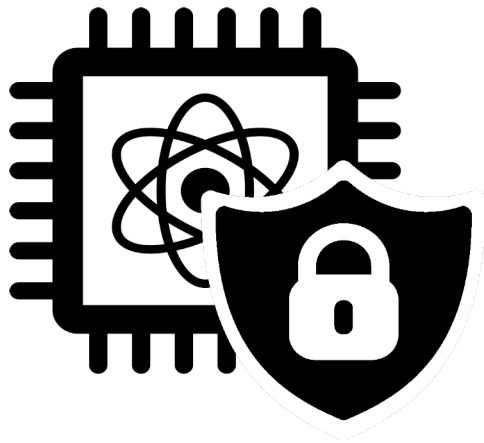
To be held November 11 and 12,
2026 at The Guild Lounge in
Scott Hall at Northwestern
University



Computer Architecture
and Security Lab (CASLAB)



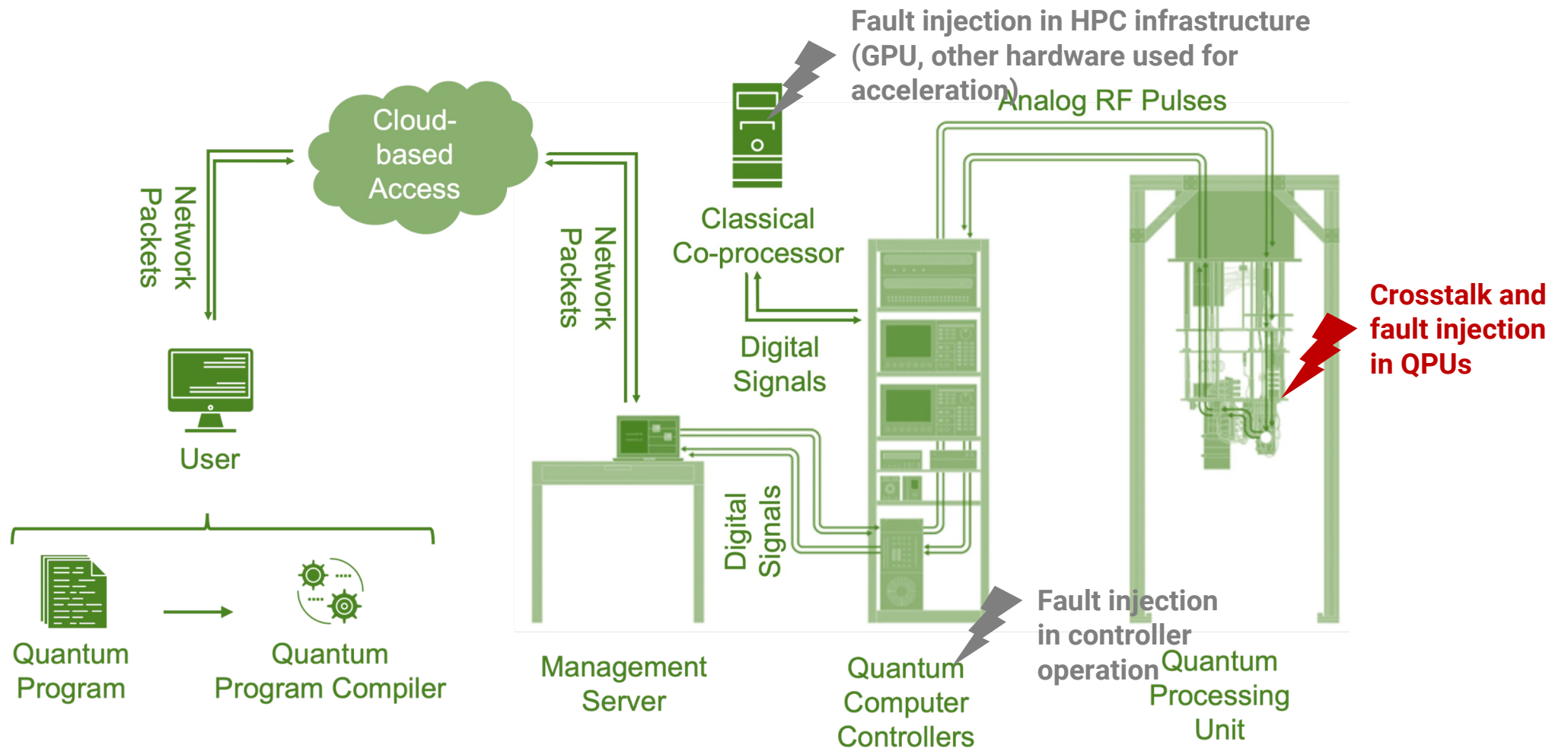
Northwestern
University



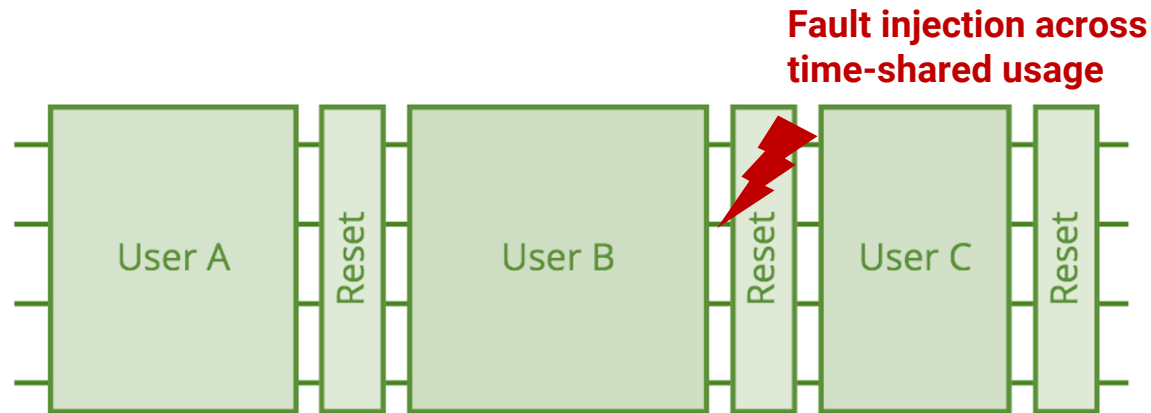
Crosstalk and Fault Injection in NISQ Quantum Computers



Crosstalk and Fault Injection in NISQ Quantum Computers



Crosstalk and Fault Injection Scenarios

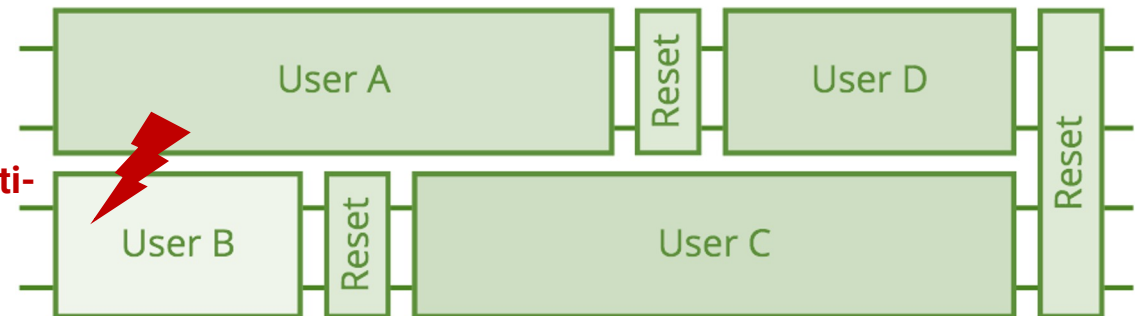


Single-tenant



No quantum computer provider publicly uses multi-tenant configuration as of 2026

Crosstalk and fault injection between multi-tenant user

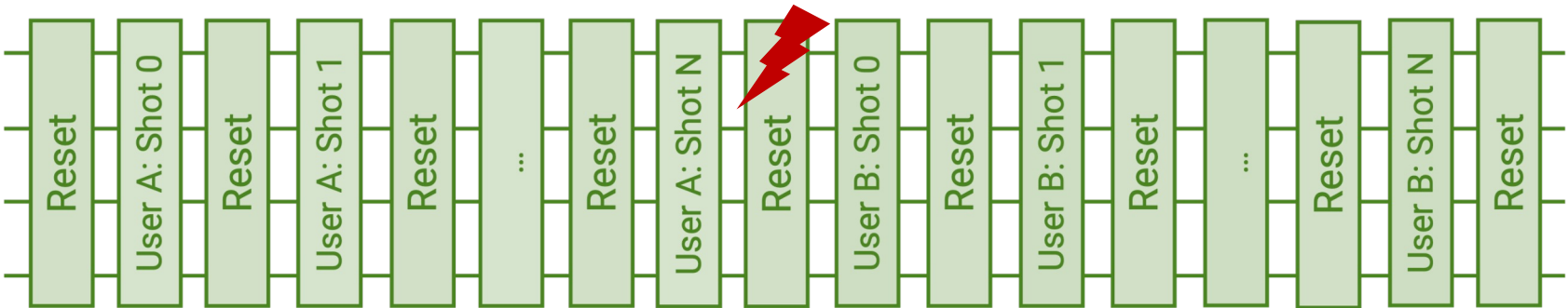


Multi-tenant



Crosstalk and Fault Injection Scenarios

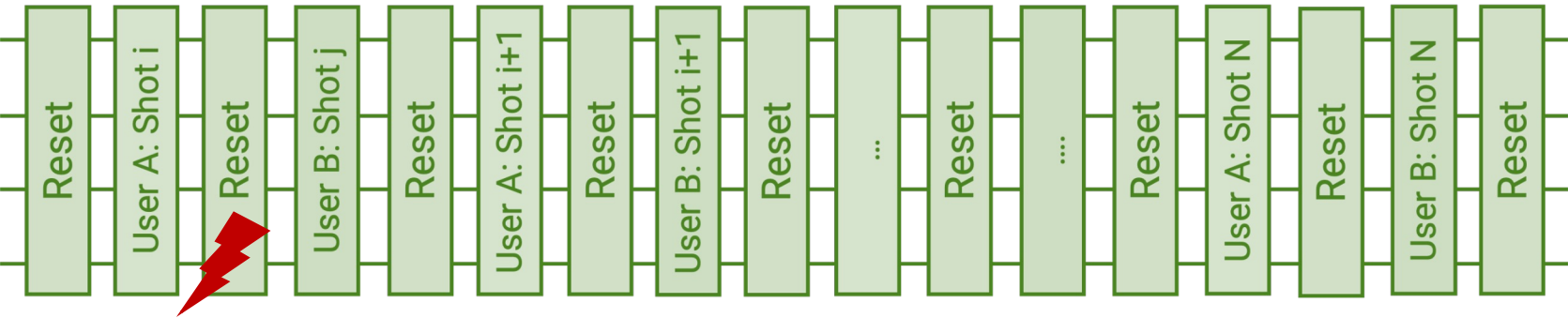
Fault injection at boundary
when users switch (affects
one shot of victim)



Single-tenant, Batch Shots



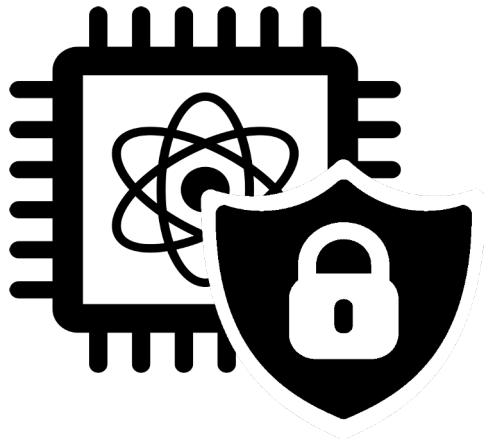
No quantum computer
provider publicly interleaves
shots of circuits as of 2026



Fault injection at each
shot execution (affects
each shot of victim)

Single-tenant, Interleave Shots

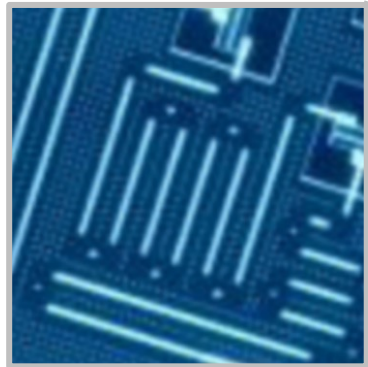
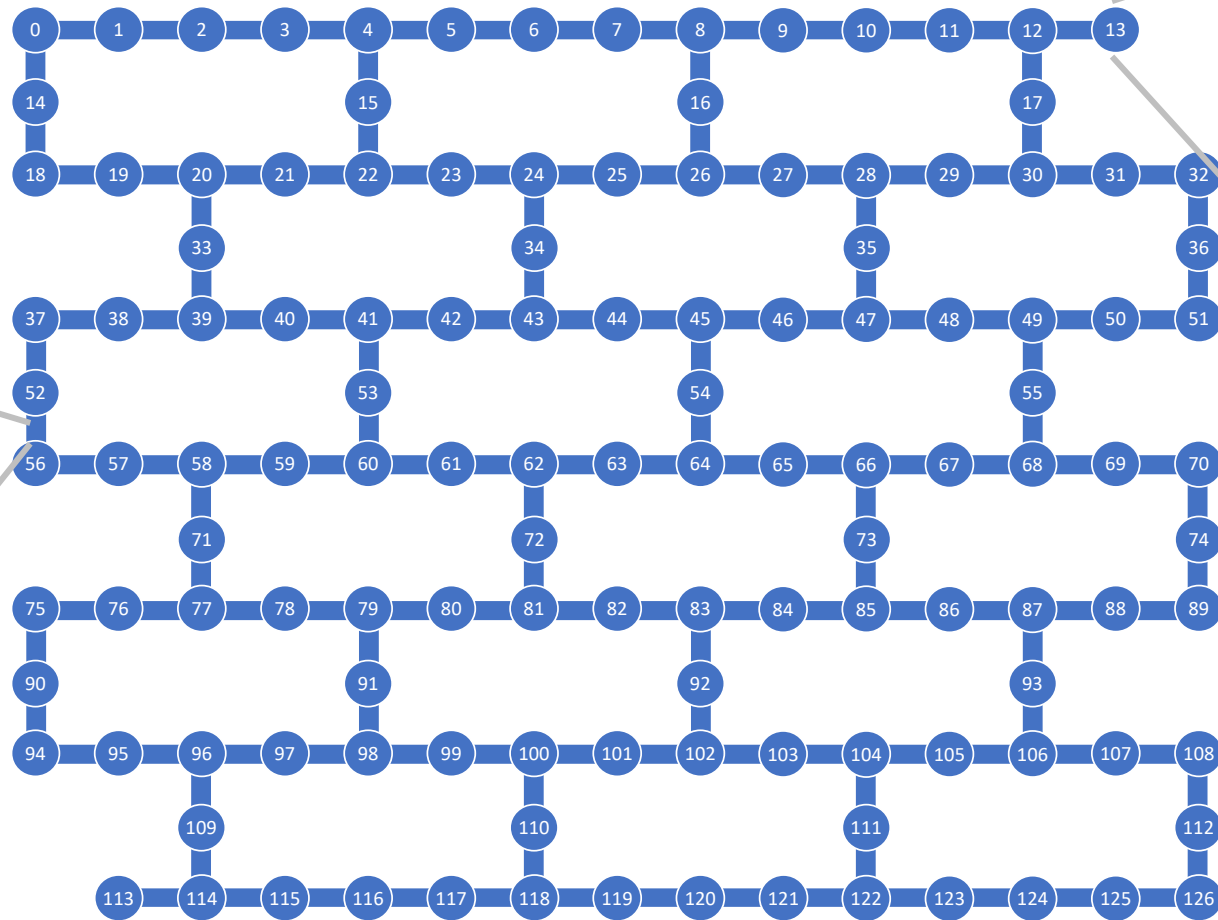




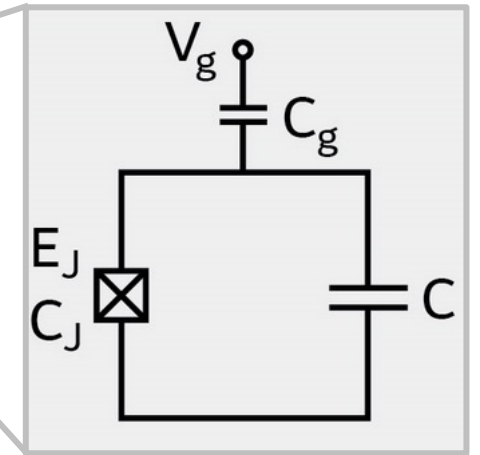
Crosstalk and Fault Injection among Qubits



Superconducting Qubit Quantum Computer Topology



A coupler,
used for 2-
qubit gate
operations



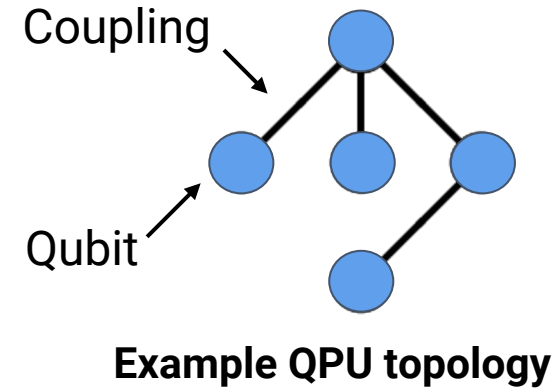
A transmon qubit,
used to store
qubit state.

Topology of IBM Quantum
Eagle R3 Processor with
topology for 127 qubits.



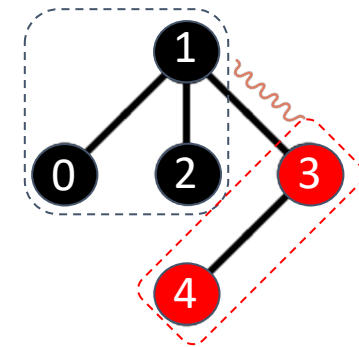
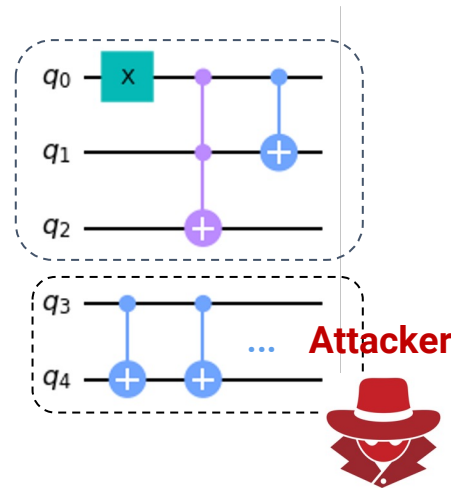
Crosstalk Attacks Among Circuits

- Crosstalk is the effect of performing computation on one or more qubits unintentionally affecting one or more other qubits
- Based on how the Qubits are arranged, signal intended for one qubit may affect other qubits through crosstalk



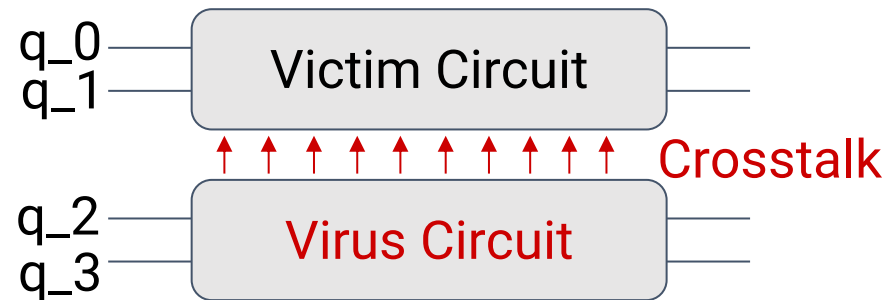
Quantum Half Adder

Series of CNOT gates



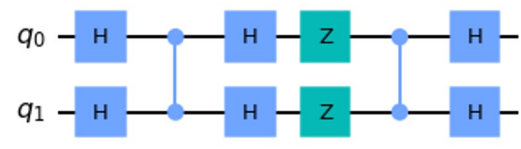
Analyzing Possible “Virus” Circuits

- Assume that victim and attacker share the same QPU



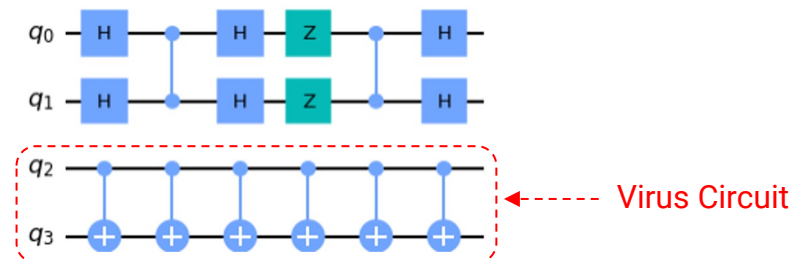
- Virus circuit aims to reduce fidelity of the victim circuit

Target Circuit: Grover's Circuit - 2-Qubits



Output Probability = P_{orig}

Grover's 2-Qubit Circuit + Virus Circuit

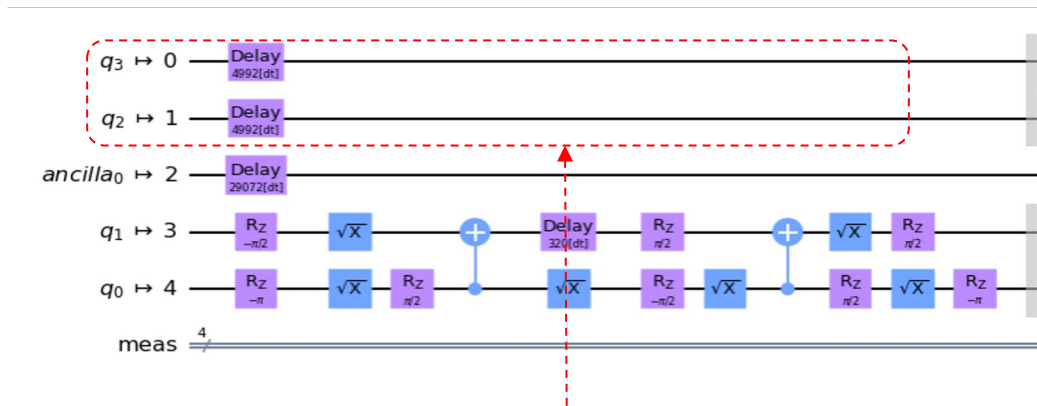


Expected Output Probability $< P_{orig}$



Attackers Need to Bypass Compiler Optimizations

- Compilers optimize away useless circuits
 - Circuit of all CNOT gates will be optimized away



Transpile function decomposes and removes the virus circuit

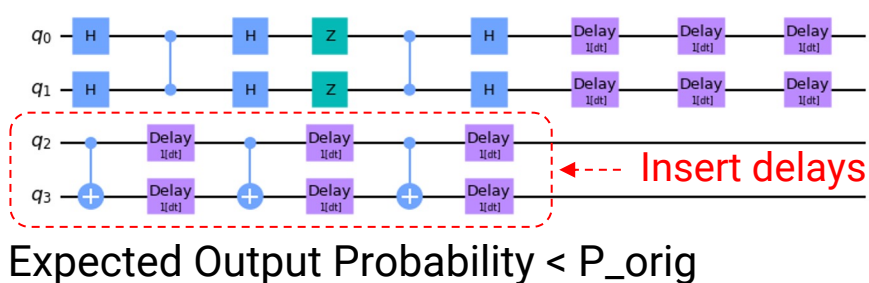
- Can develop “viruses” that have different sets of gates to avoid being optimized away



Bypassing Compiler Optimizations

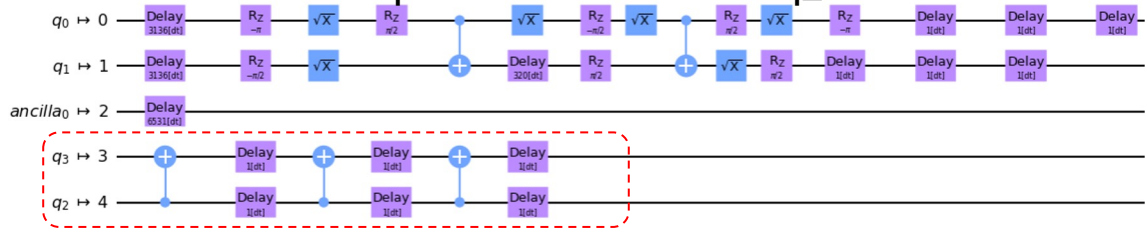
- Virus circuit with delays inserted

Grover's 2-Qubit Circuit + Proposal for Virus Circuit

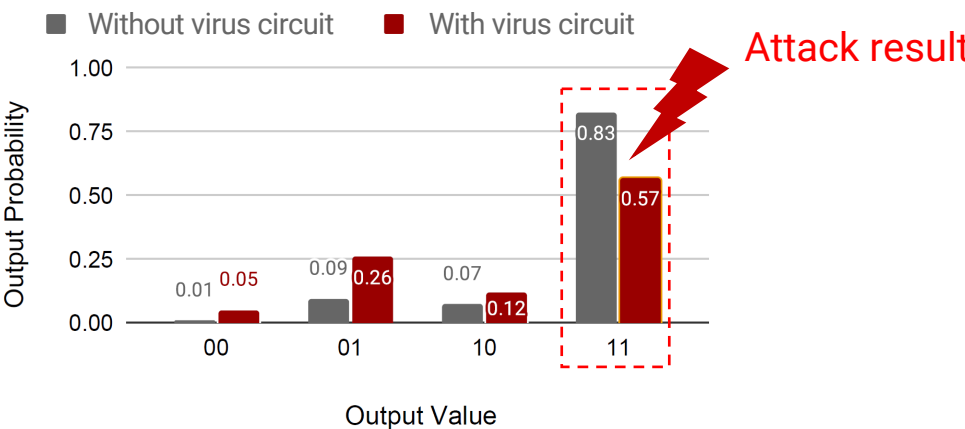


Grover's 2-Qubit Circuit + Virus Circuit

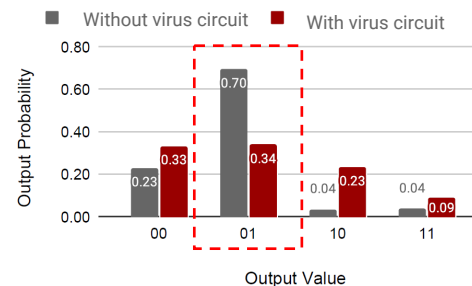
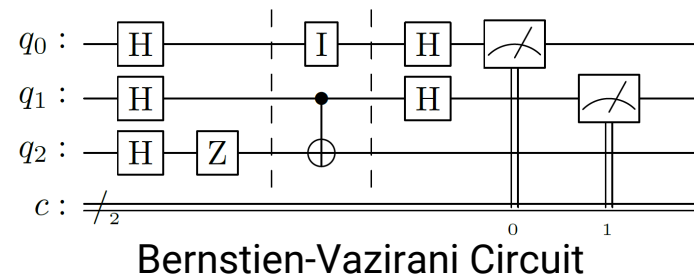
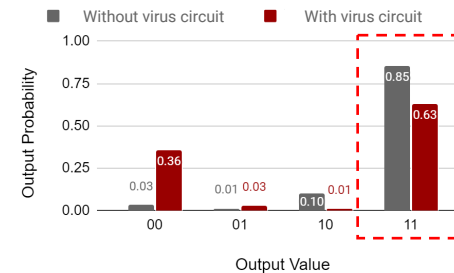
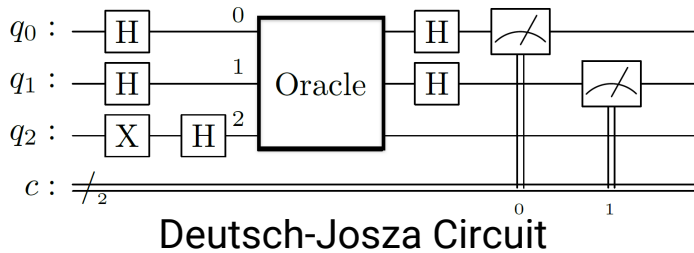
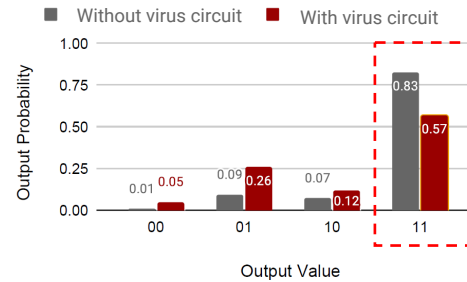
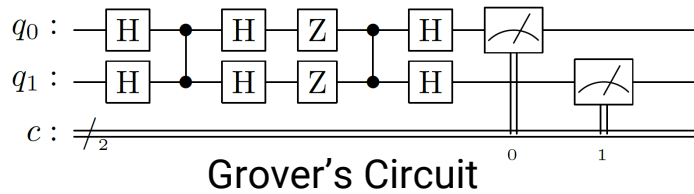
Transpiled for Device: ibmq_lima



Transpile function could not decompose this virus circuit



Changing Output Probability of Victim Circuits



Grover's Algorithm:

- Provides Quadratic Speed up in Unstructured Search
- The attack here is to lower the correct output probability and increase probability of random output
- On a large scale, applications like traveling salesman problem, deadlock prevention could be attacked

Deutsch-Jozsa Algorithm:

- Determines whether a given Oracle is constant or balanced
- The attack here is to identify balanced oracle as a constant oracle

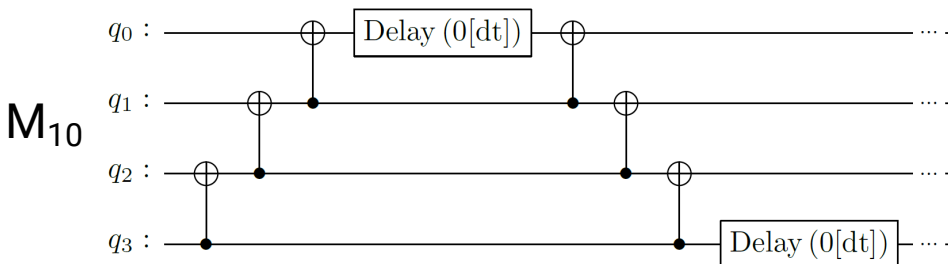
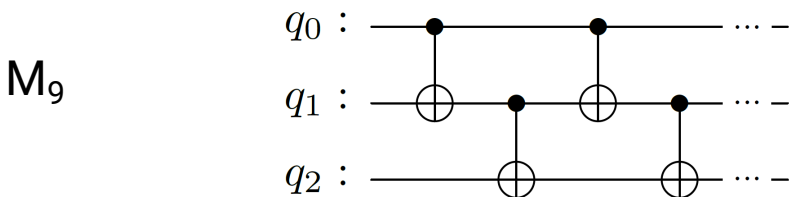
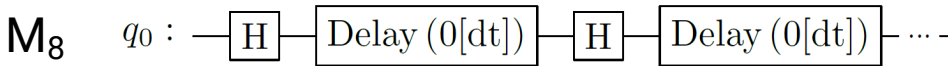
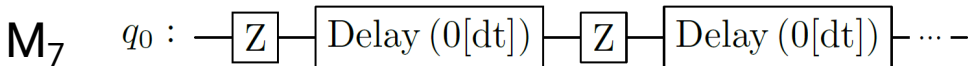
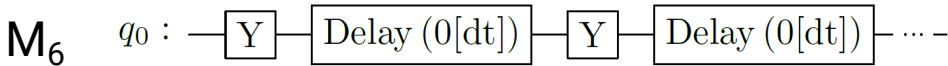
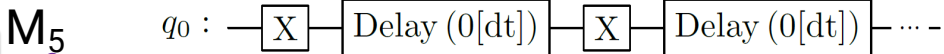
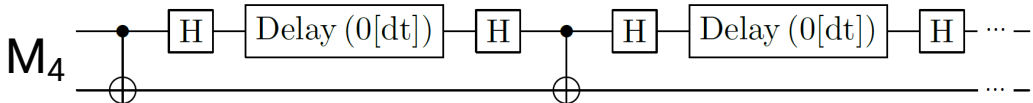
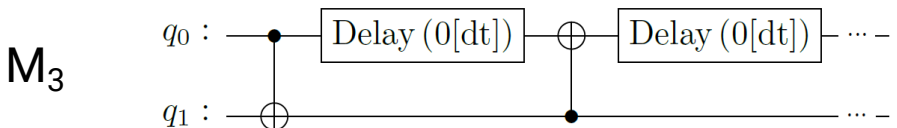
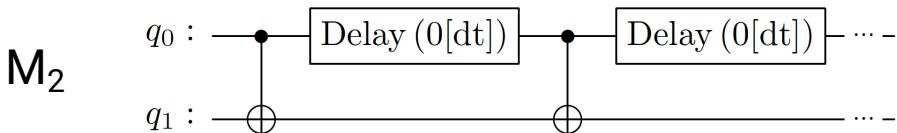
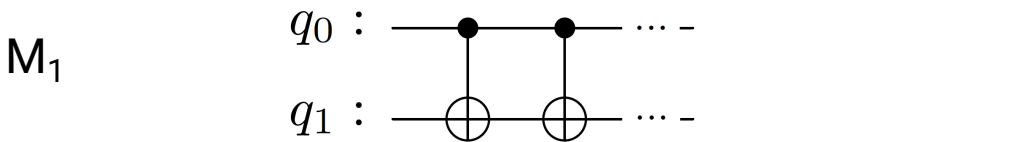
Bernstein-Vazirani Algorithm:

- Finds out a hidden string with a single query to Oracle
- The attack here is retrieving incorrect secret string at the output



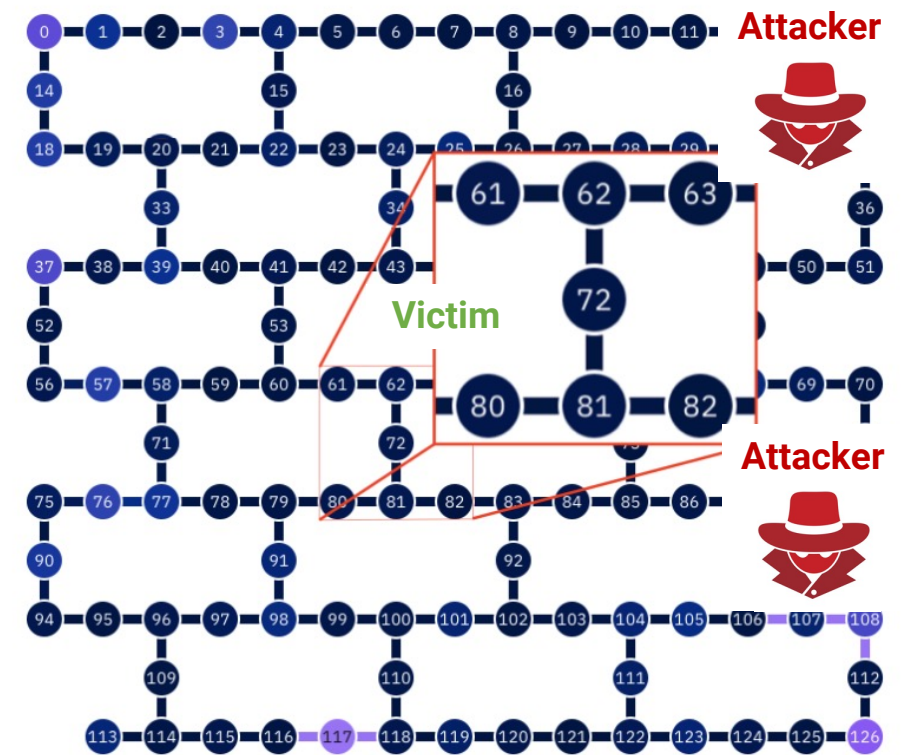
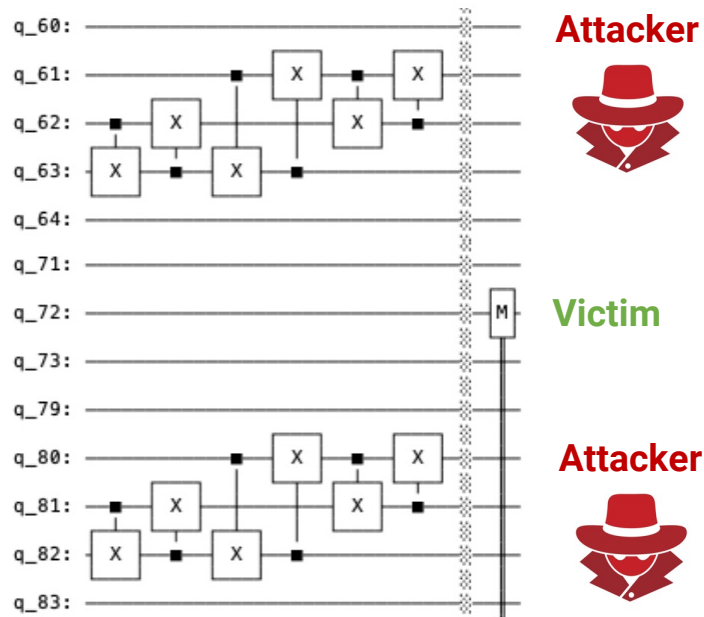
Candidate “Virus” Circuits

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



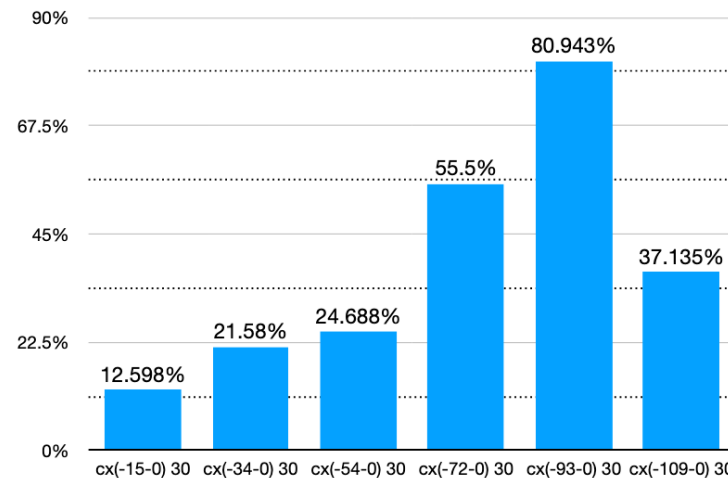
Double-Sided Crosstalk Attacks

- Extension of the crosstalk attack is to perform the attack by leveraging qubits on two sides of the victim qubit:

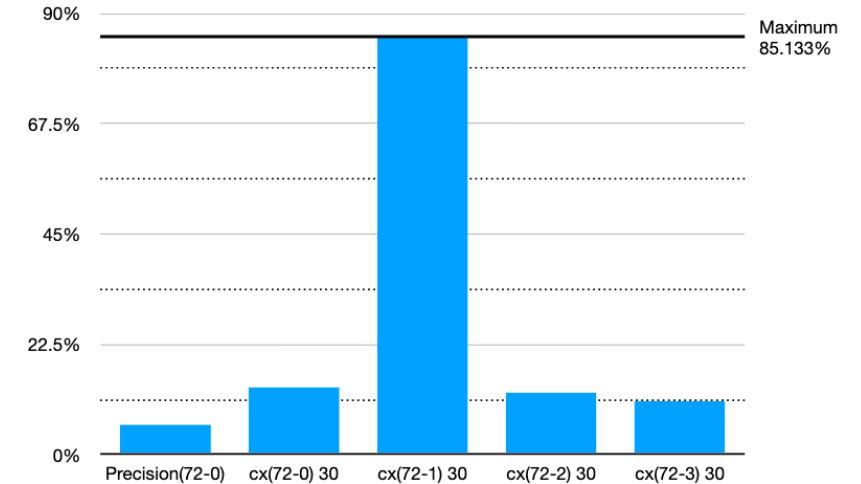


Double-Sided Crosstalk Attack Success Rates

- On IBM Sherbrooke, 30 *CNOT* gates around victim qubit 72 can cause the victim to flip from $|0\rangle$ to $|1\rangle$:



- As well as $|1\rangle$ to $|0\rangle$:

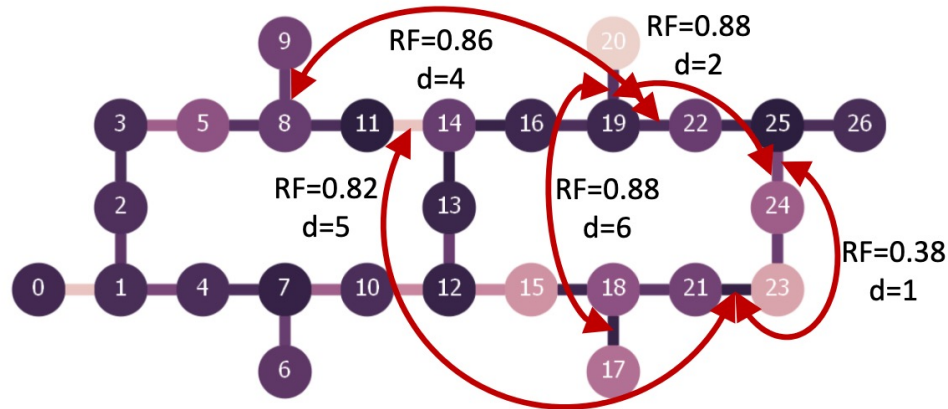


- Attacks required 40,000 CNOT operations, which is rather significant

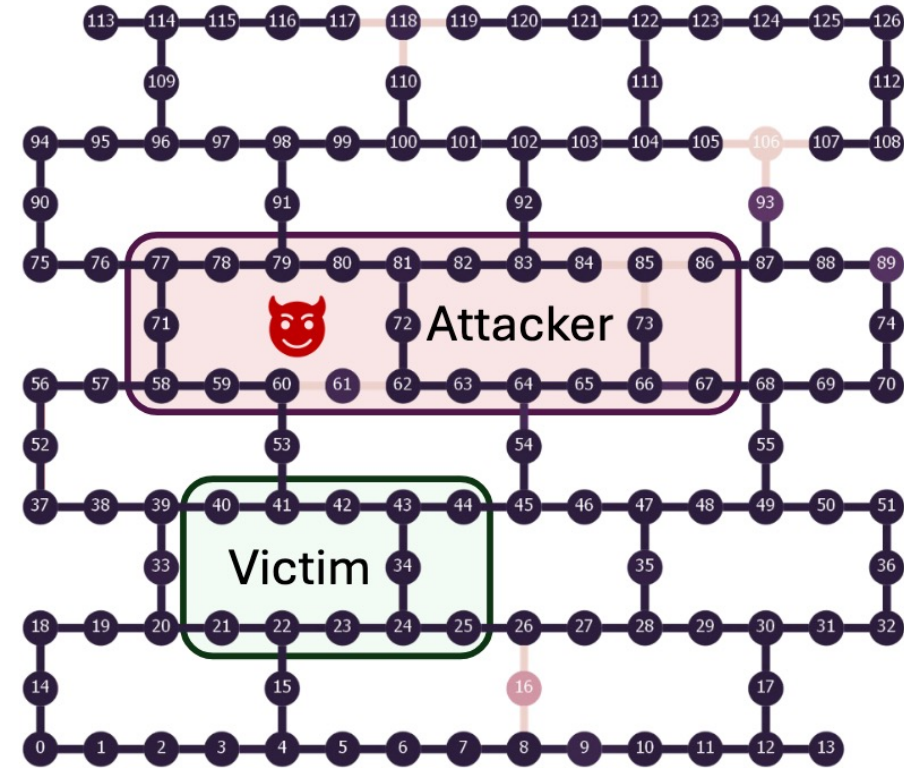


High Crosstalk Coupling Pairs

- Beyond adjacent qubits and couplings, certain couplings display higher crosstalk than others, e.g., high crosstalk pairs on IBM Hanoi:

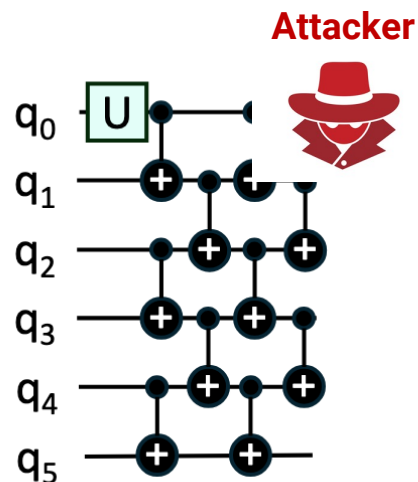
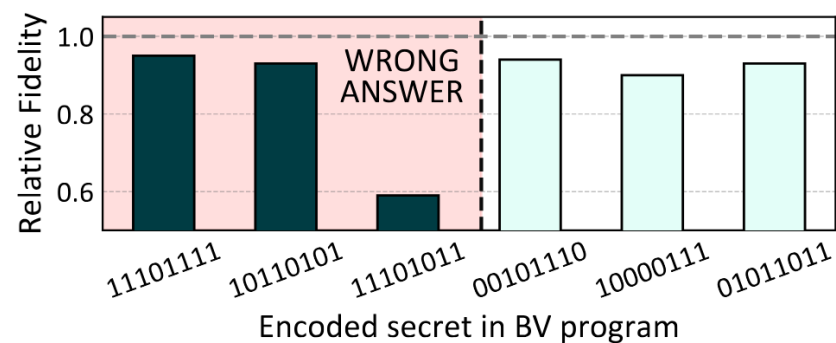
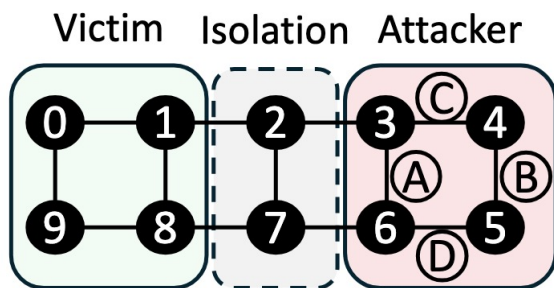


- Victim and attacker can 1 or 2 couplings away:



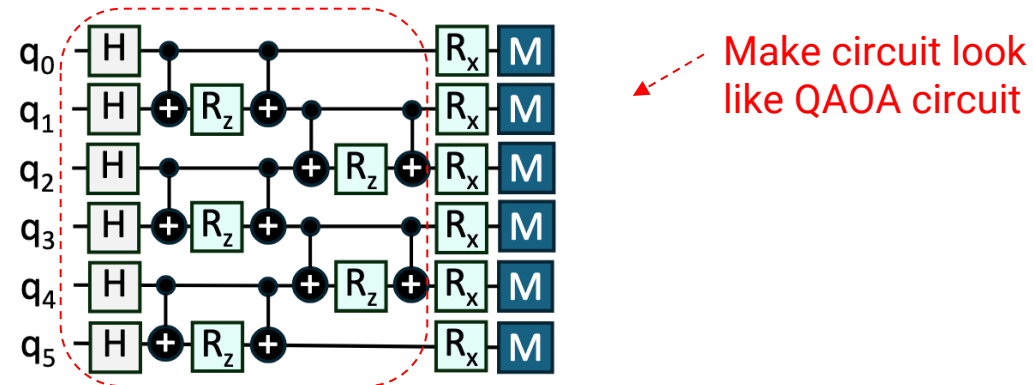
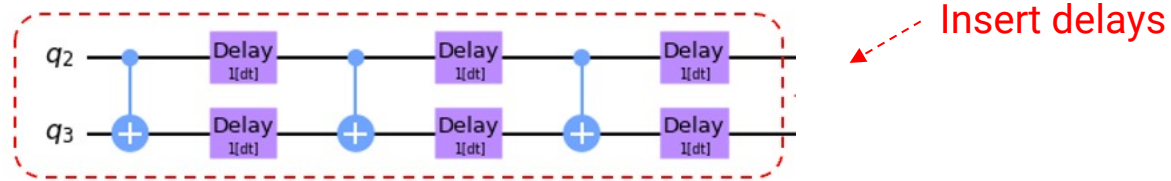
Example Attacks on BV Circuits

- Attacker leverages repeated *CNOT* gates to induce noise, even if there is isolation:



Evolution of Obfuscation of Attacker Circuits

- Hiding the attacker circuit can help make the attacks more stealthy:

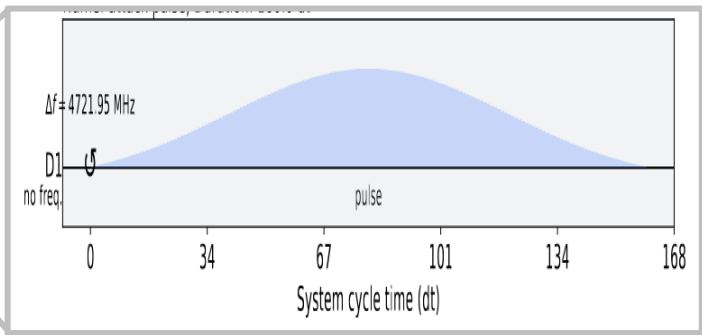
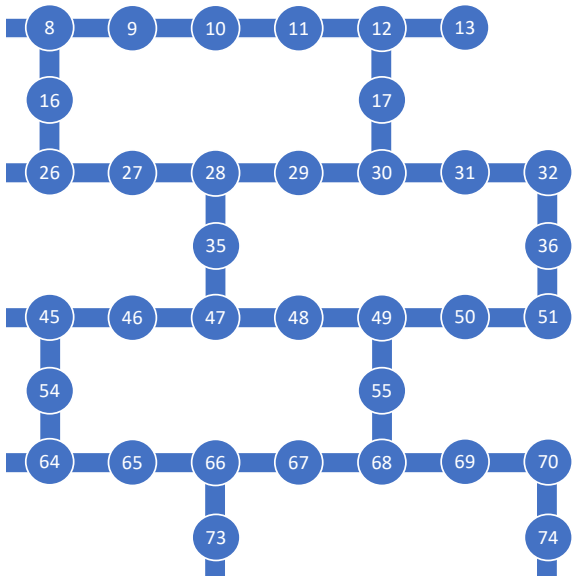


Reference:

Deshpande, et al. (HOST 2022)
Kumar, et al. (arXiv 2025)

Novel Crosstalk Attacks with Custom Control Pulses

- In superconducting qubit quantum computers, each qubit has its own frequency and other parameters:



Qubit control pulse for X gate

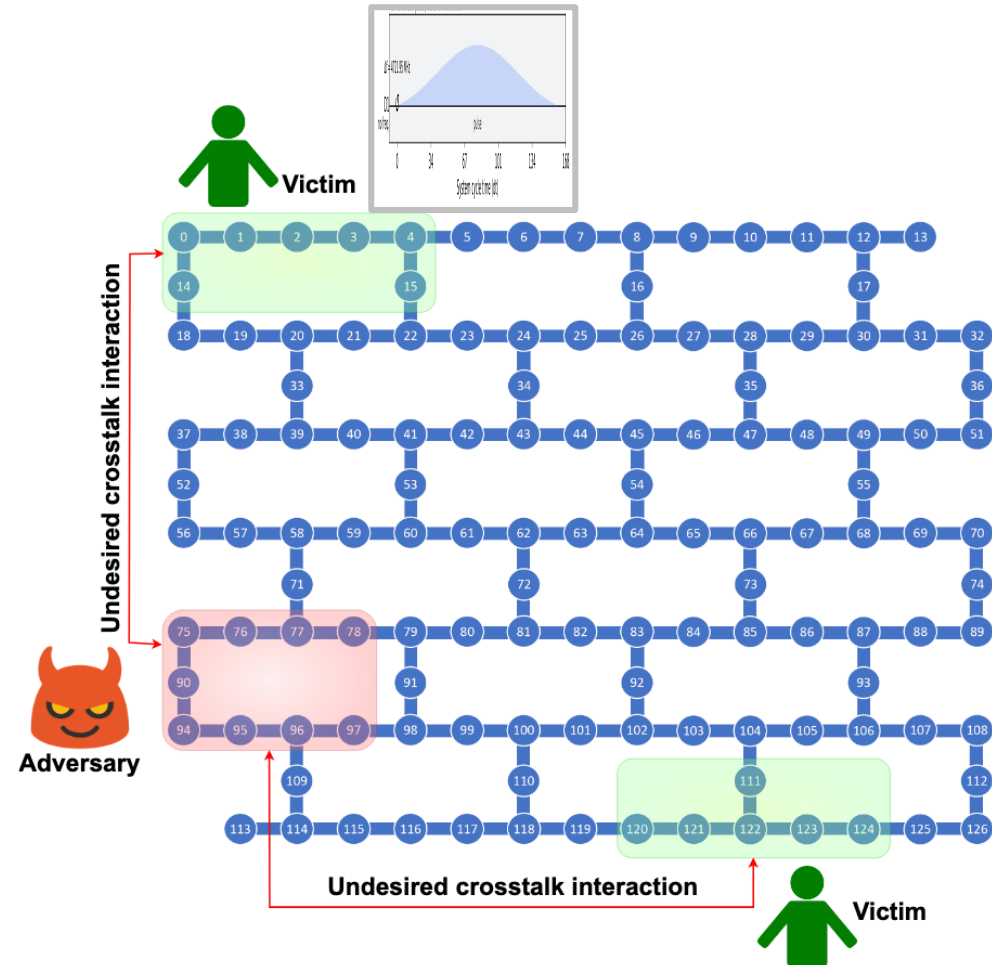
- Various qubit properties:

Qubit	Energy relaxation time T1 (μs)	Dephasing time T2 (μs)	Frequency (GHz)	Readout error rate
Q0	98.33551265	46.82808058	4.641200919	5.50000e-2
Q1	66.80352570	84.08716319	4.719992563	6.05e-2
Q2	77.96055113	88.27547132	4.761962111	4.04999e-2
Q3	93.81392649	86.04122557	4.687003753	5.04999e-2
Q4	57.44885729	40.31605568	4.923978085	4.00000e-2



Configuring Custom Control Pulse

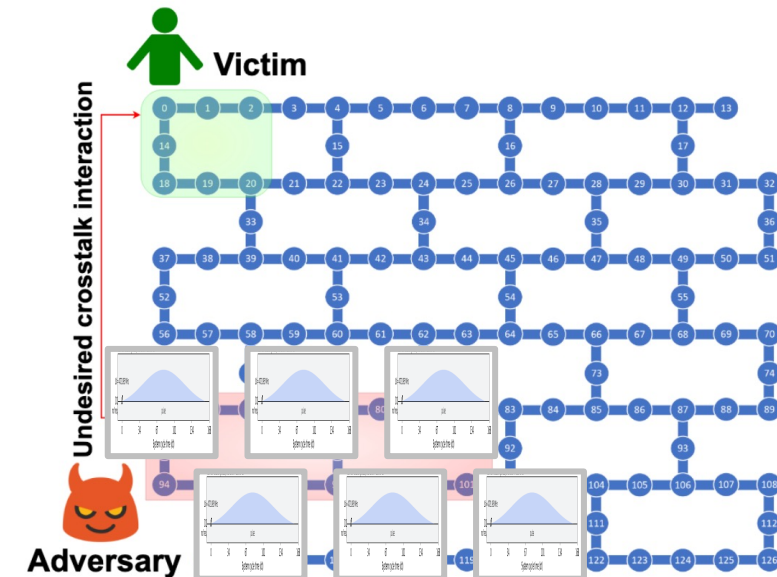
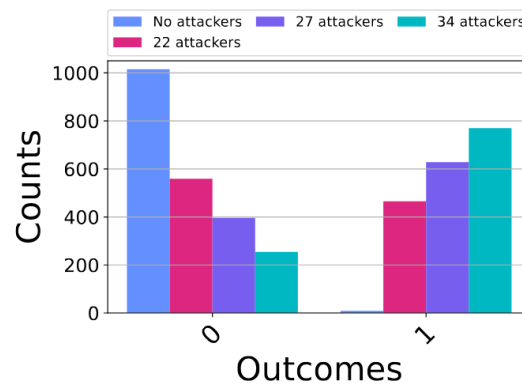
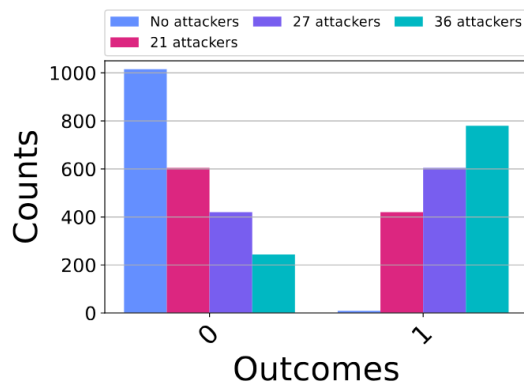
- Qiskit Pulse is one library that allows for configuration of custom pulses, usually to explore novel algorithm design
- **But can configure wrong pulse on purpose to explore crosstalk effects**
- *E.g. executing pulse for qubit 0 on qubit 75 has no effect on qubit 75, but may affect qubit 0 through crosstalk*



Long-Distance Crosstalk Attacks

- Repeating the “wrong” control pulses on many distant qubits can lead to disruption of the victim qubit and circuits running on victim's qubits:

- Attack results at distance 13 and 17:



Stealthy SWAPs

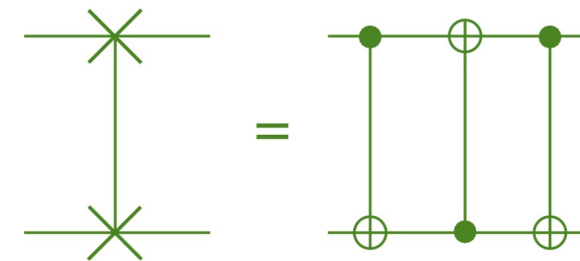
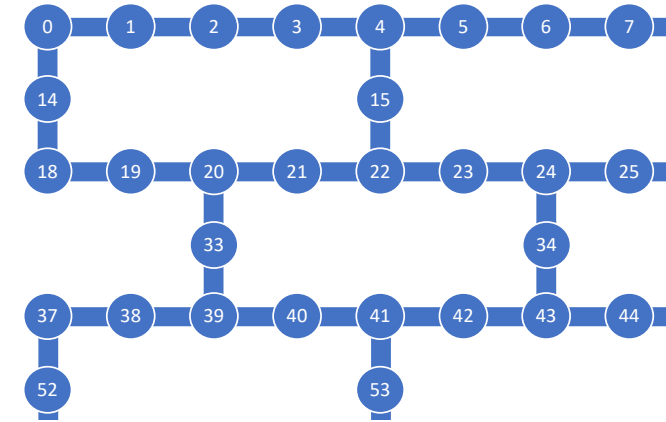
The limited connectivity between qubits in existing quantum computers necessitates the use of SWAP operations for 2-qubit gates between qubits that are not directly connected.

- This incurs additional computational costs and introduces error accumulation.
- In a multi-tenant computing scenario, adversaries can exploit these connectivity constraints by strategically occupying specific qubit



Aside: What is a SWAP Gate

- 2-qubit gates can only execute between qubits that are connected by a coupler
- $\text{CNOT}(q1, q2)$ is possible in the topology on the side, but $\text{CNOT}(q1, q3)$ is not
- Need to add a SWAP gate to swap $q2$ and $q3$
- SWAP gate: swaps state of two qubits via a sequence of CNOT gate operations

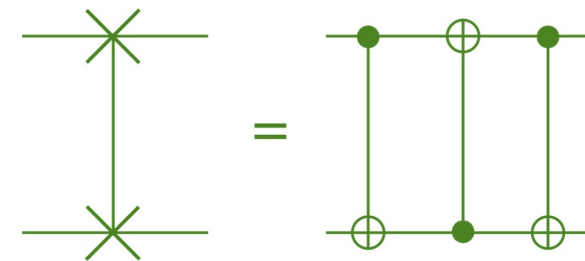


Aside: What is a SWAP Gate

- SWAP gate can be implemented with 3 CNOT gates, assume qubit states A and B:
 1. Initial state is $|A, B\rangle$
 2. Apply 1st CNOT gate, $\text{CNOT}(|A\rangle, |B\rangle) \rightarrow |A, A \oplus B\rangle$
 3. Apply 2nd CNOT gate, $\text{CNOT}(|A \oplus B\rangle, |A\rangle) \rightarrow |A \oplus B, |A \oplus A \oplus B\rangle \rightarrow |A \oplus B, B\rangle$
 4. Apply 3rd CNOT gate, $\text{CNOT}(|B\rangle, |A \oplus B\rangle) \rightarrow |B, |B \oplus A \oplus B\rangle \rightarrow |B, A\rangle$
 5. Final state is $|B, A\rangle$

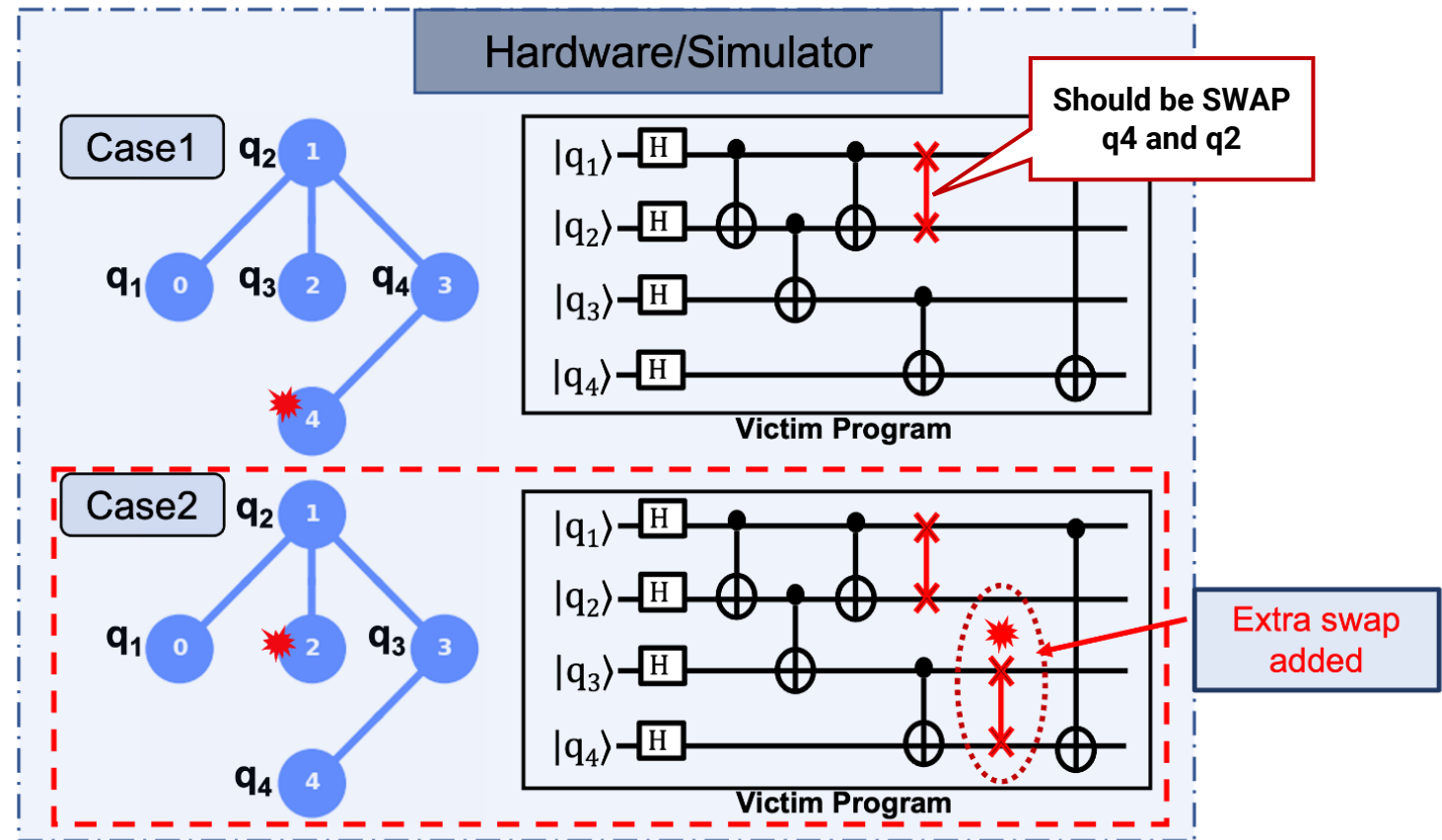
SWAP gates introduce error:

- CNOT can be 99.5% fidelity
- SWAP = 3*CNOT = 98.5% fidelity



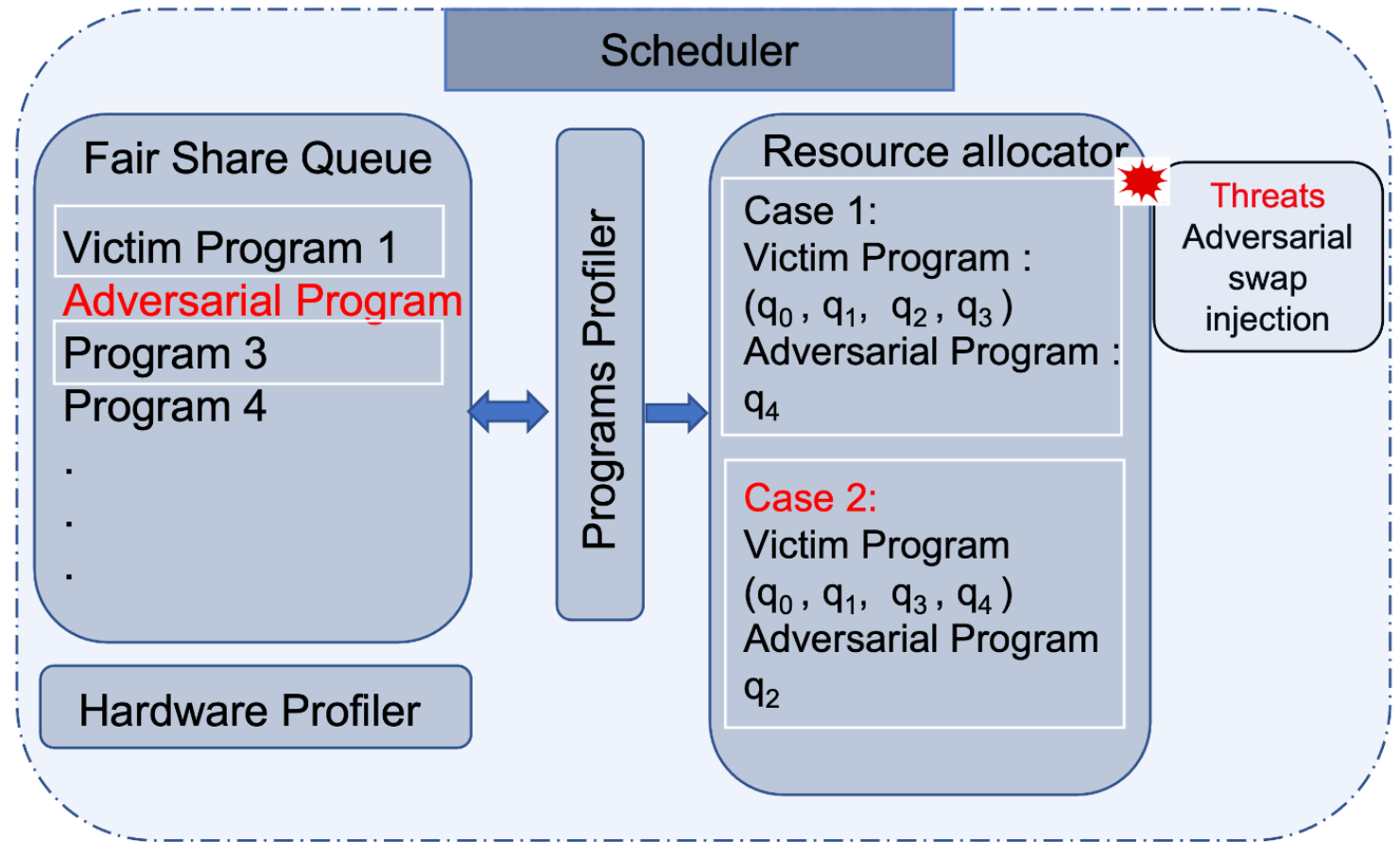
Stealthy SWAPs

- Based on what qubits are assigned to attacker and victim, victim may have to perform more SWAP gates operations



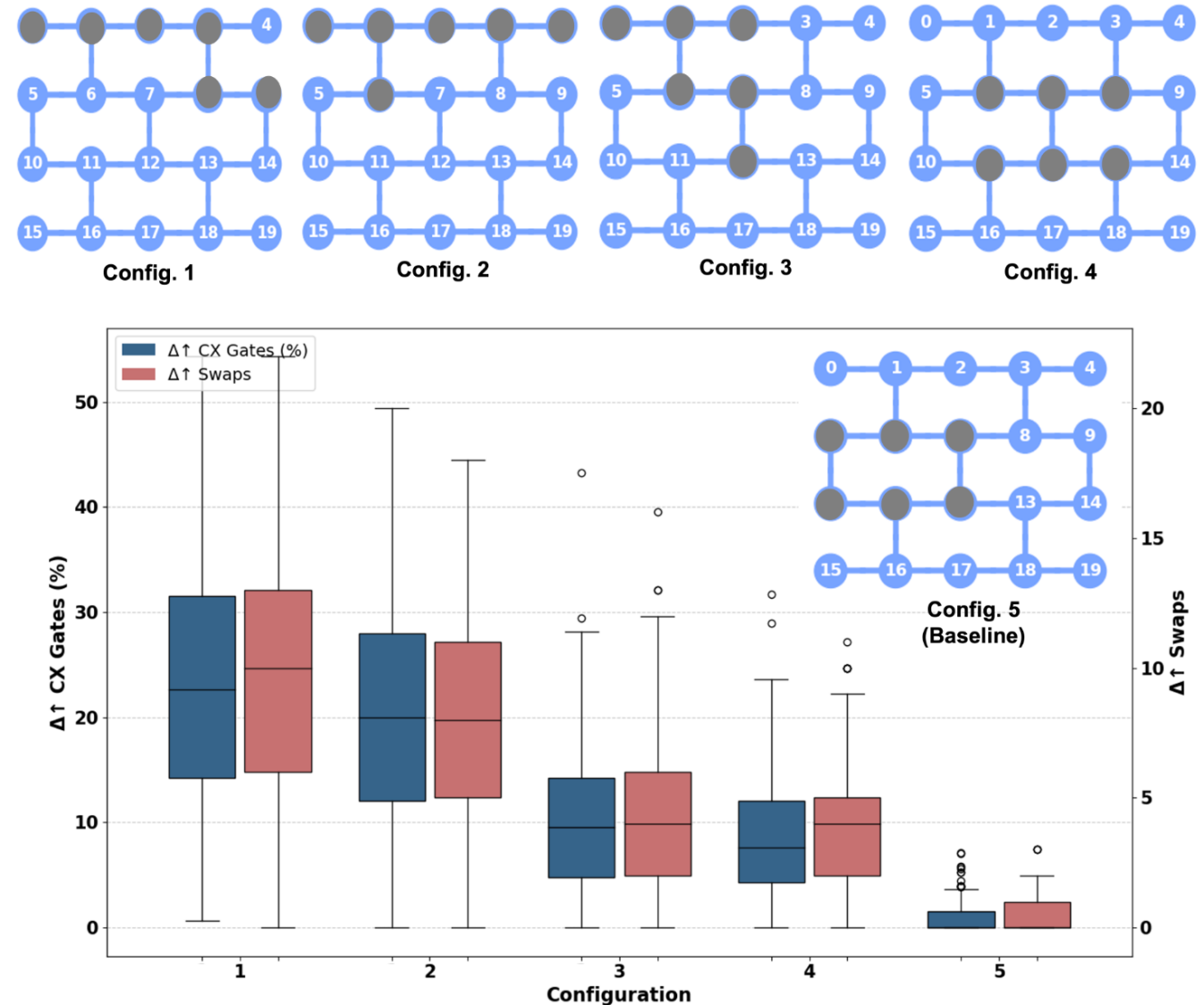
Executing Stealthy SWAPs Attack

- Attack focuses on modifying the scheduling of different quantum circuits in a multi-tenant system



Attack Results

- If attacker occupies specific qubits, it will force victim to other qubits and require more SWAPS in victim
- More SWAPS results in lower fidelity of the computation, causing a type of fault injection attack
- But does require attacker to occupy specific qubits, not possible today



Crosstalk Summary and Outlook

Many attacks have been demonstrated:

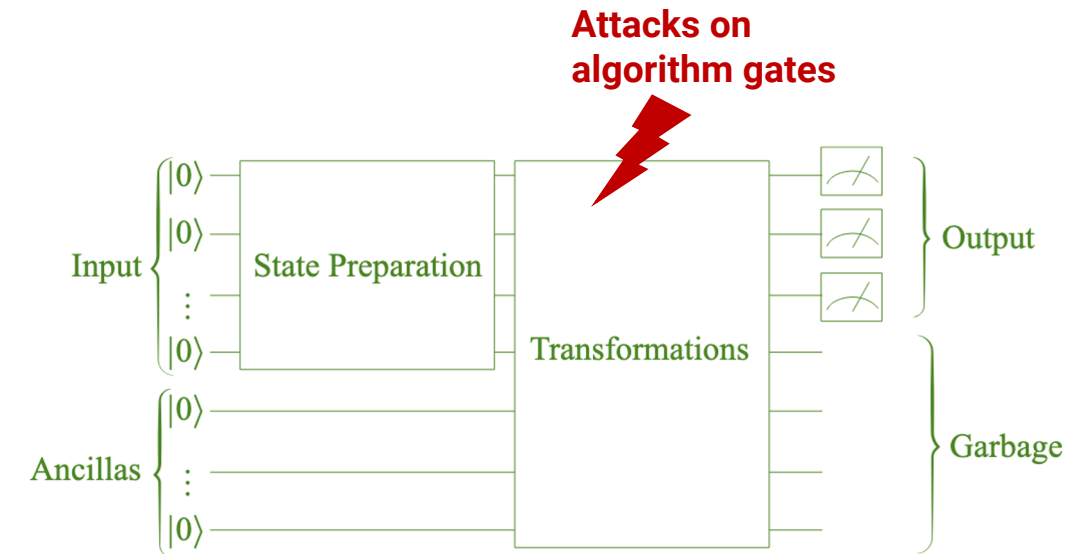
- Single-side crosstalk (since about 2021)
- SWAP attacks (2023)
- Crosstalk with custom pulses (since about 2024)
- Double-side crosstalk (2025)

Various defenses have been proposed in parallel:

- Quantum computer antivirus (since about 2021)
- Others, e.g., isolation or scheduling changes

Future directions in this research:

- Cross chiplet crosstalk attacks
- Integration with multitenancy

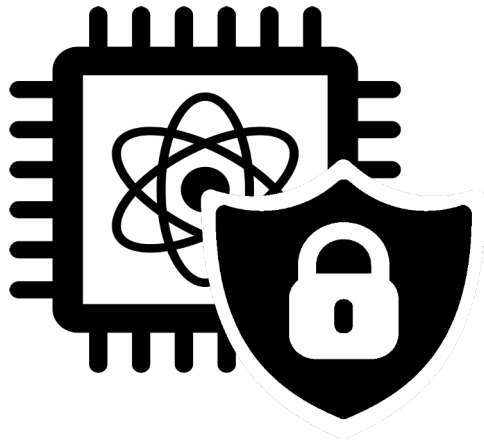


	Heron (5K)	Flamingo (5K)	Flamingo (7.5K)	Flamingo (10K)	Flamingo (15K)	Starling (100M)	Blue Jay (1B)
	Error mitigation	Error mitigation	Error mitigation	Error mitigation	Error mitigation	Error correction	Error correction
	5k gates 133 qubits	5k gates 156 qubits	7.5k gates 156 qubits	10k gates 156 qubits	15k gates 156 qubits	100M gates 200 qubits	1B gates 2000 qubits
	Classical modular	Quantum modular	Quantum modular	Quantum modular	Quantum modular	Error corrected modularity	Error corrected modularity
	Up to 133x3 = 399 qubits	Up to 156x7 = 1092 qubits	Up to 156x7 = 1092 qubits	Up to 156x7 = 1092 qubits	Up to 156x7 = 1092 qubits		



No quantum computer provider publicly uses multi-tenant configuration as of 2026

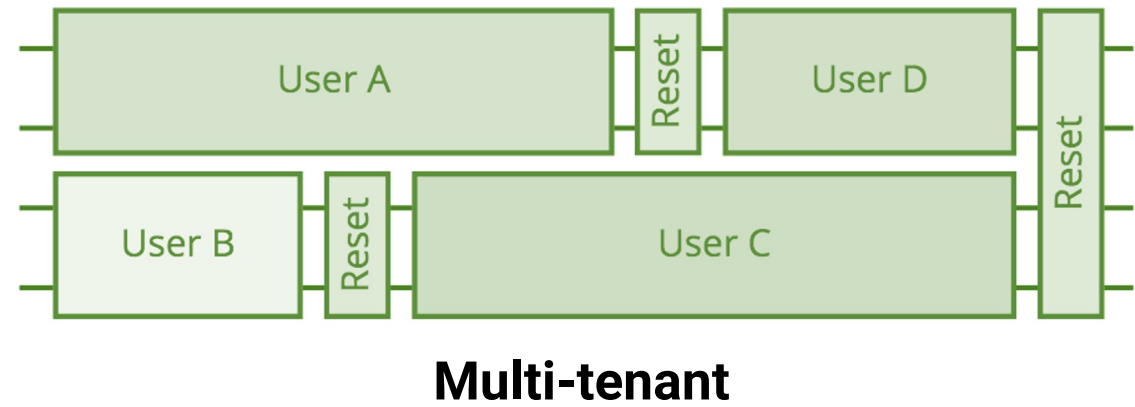
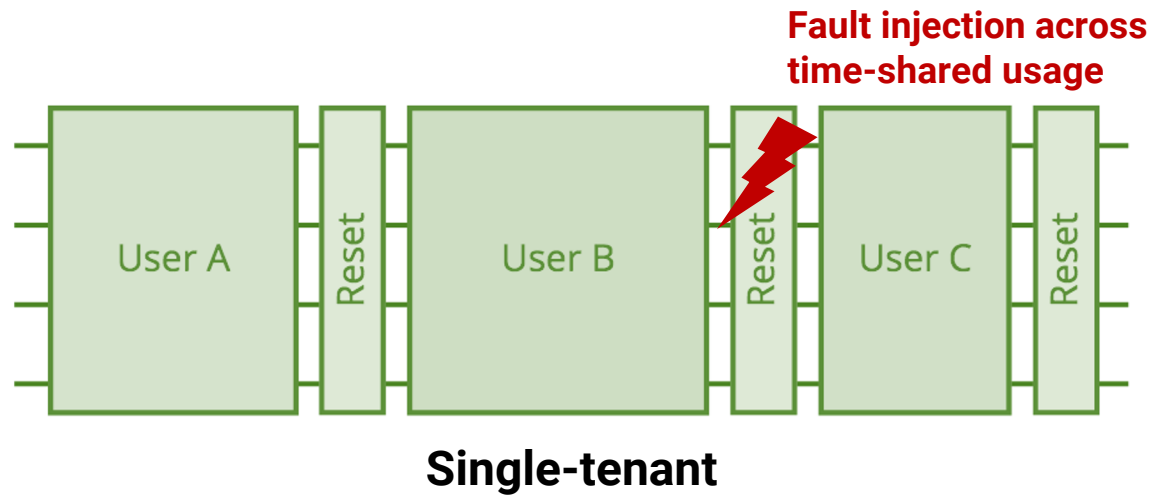




Fault Injection in Reset Gates



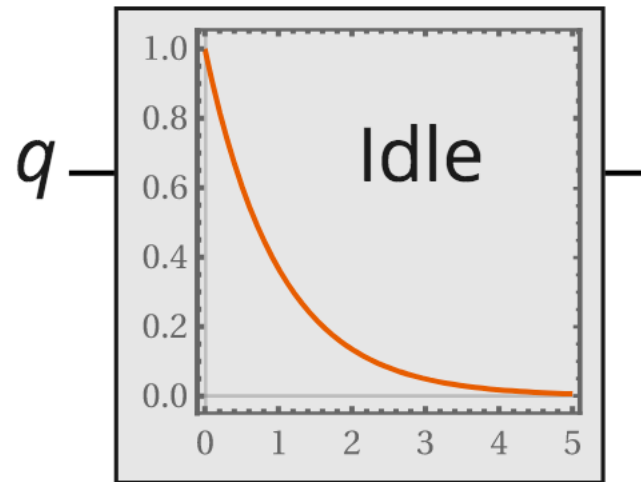
Crosstalk and Fault Injection Scenarios



What is a Reset Gate?

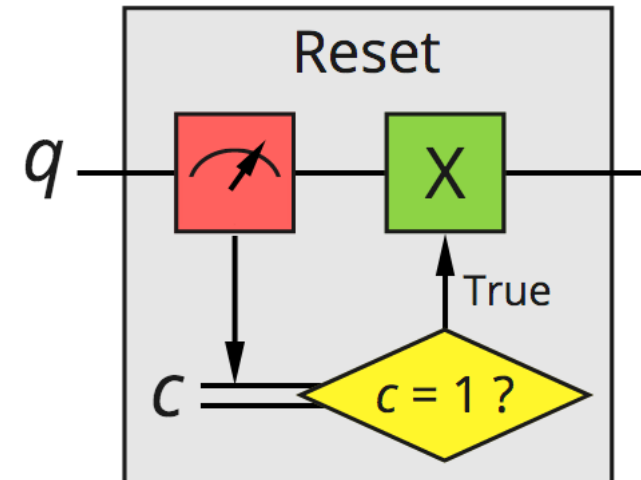
Thermalization ($250\mu\text{s} - 1\text{ms}$)

- Good: Low state retention
- Bad: Poor scaling with T



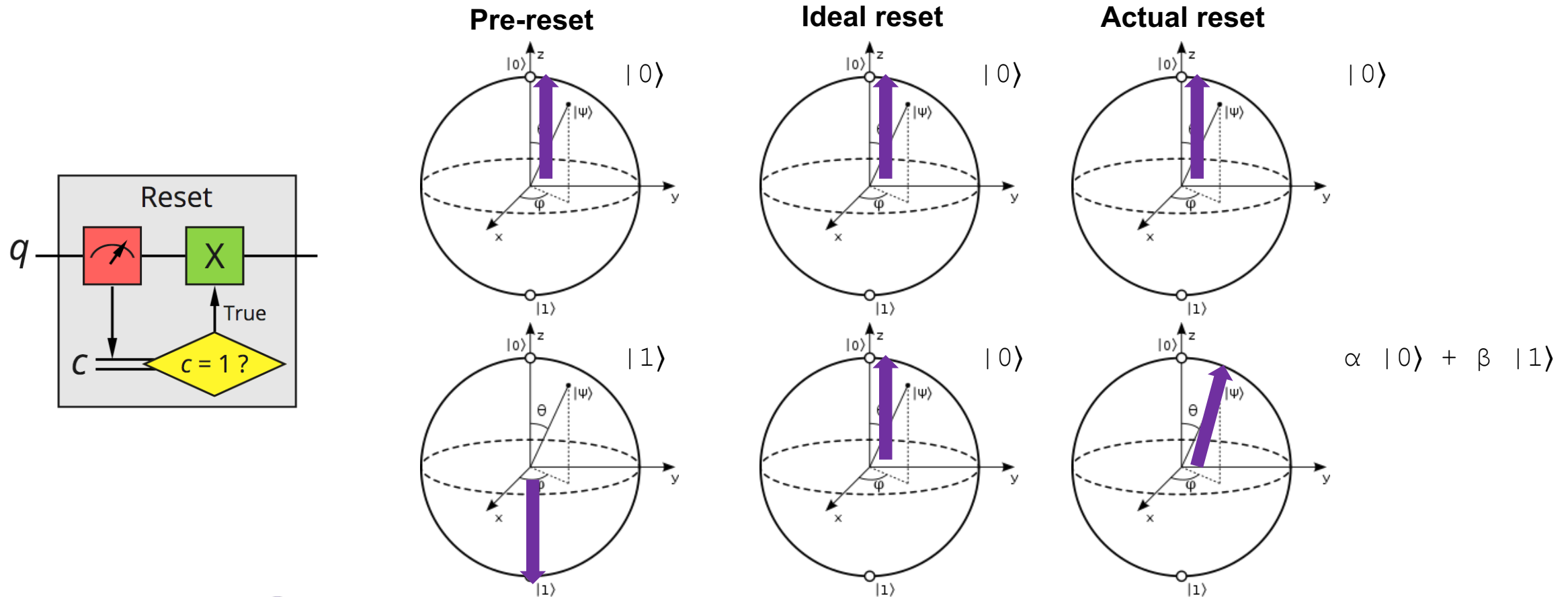
Active reset ($1\mu\text{s}$)

- Good: Fast and scales well
- Bad: Detectable state leakage



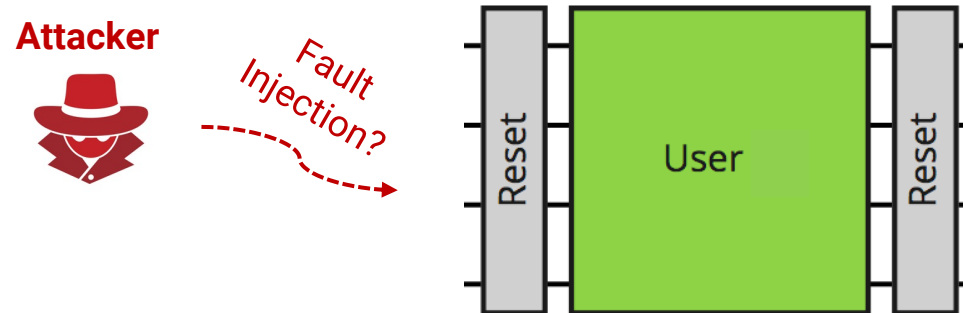
Behavior of Reset Gates

- Observed reset gate behavior on superconducting qubit quantum computers:

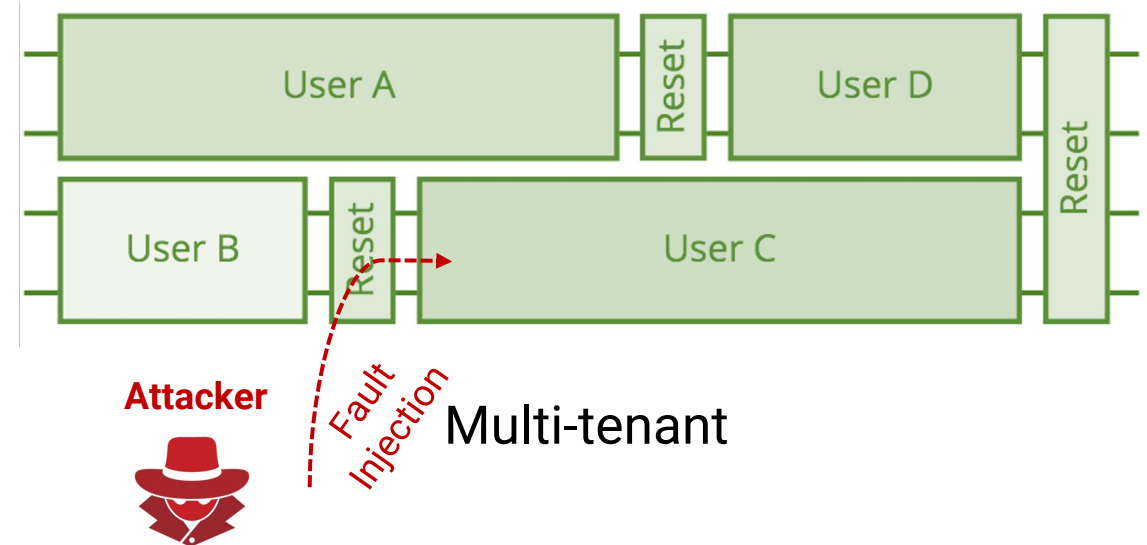
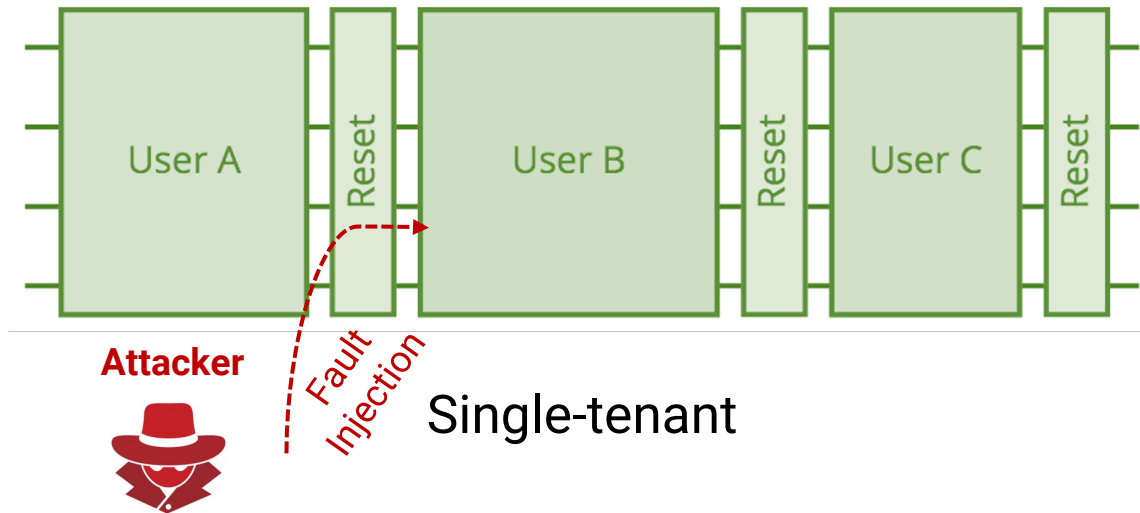


Affecting Initial Qubit State When Reset Gates are Imperfect

- Incorrect operation of the reset gate can create information leaks for user programs
- If attacker runs before victim, could cause incorrect initial state, possibly affecting the computation



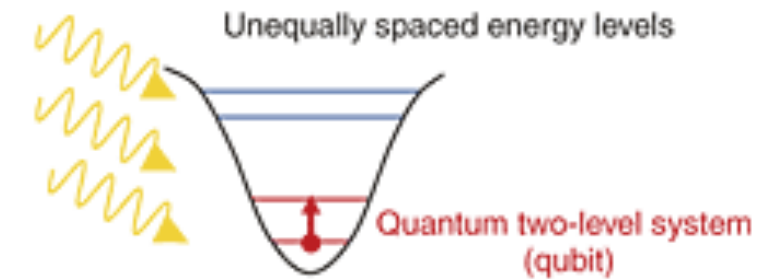
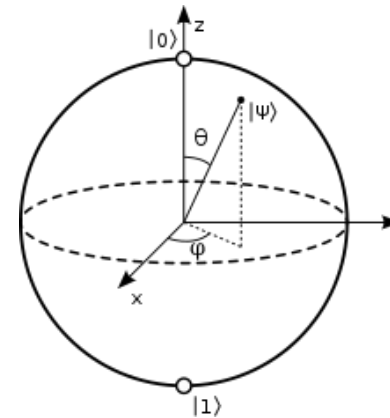
Affecting Initial Qubit State When Reset Gates are Imperfect



Revisiting Qubit Definition

Qubit: basic element of quantum computation

- Classical bits: 0 and 1
- Qubits: superposition of 0 and 1
- Abstraction of a two-state quantum-mechanical system:
 - $|0\rangle$ Ground state
 - $|1\rangle$ First excited state

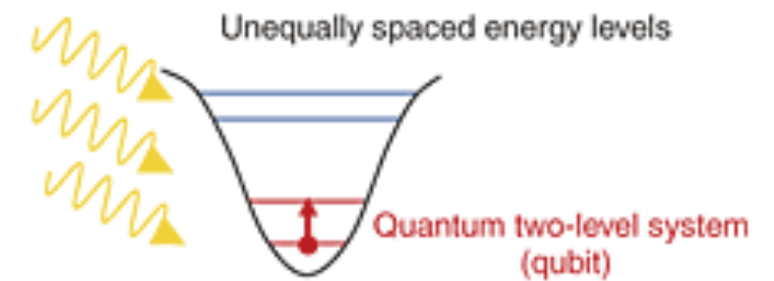


However, the physical realizations of qubits allow for states with higher energies



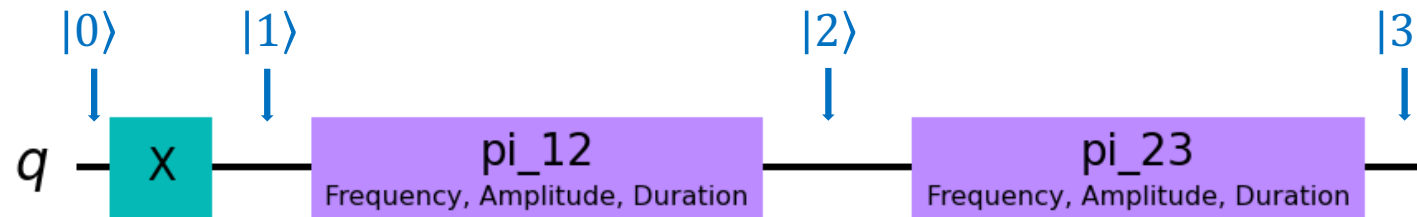
The Π Gate

- The Π gate is used to excite the state from the lower to higher energy state
- Gate $\Pi_{g,e}$ exchanges the amplitudes on two energy levels:
 - If $|\psi\rangle = a_g|g\rangle + a_e|e\rangle$ then $\Pi_{g,e}|\psi\rangle = a_e|g\rangle + a_g|e\rangle$
- Note, the X gate is also the $\Pi_{0,1}$ gate that can excite $|0\rangle$ to $|1\rangle$, and also can change the state from $|1\rangle$ to $|0\rangle$



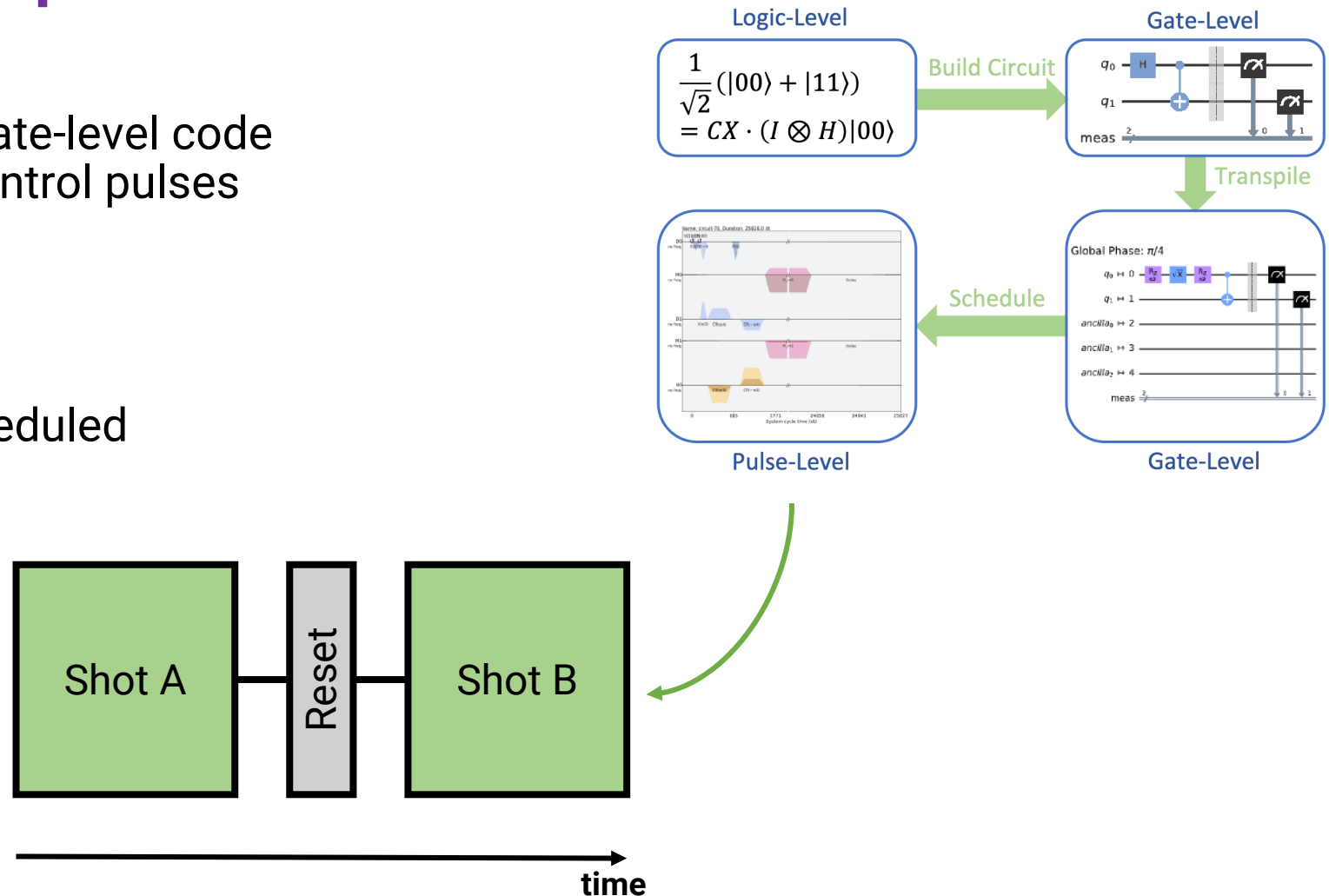
Setting Higher Energy States

- IBM Quantum, custom pulse gates are executable, and thus higher energy states may be obtained
 1. Define $\Pi_{1,2}$ and $\Pi_{2,3}$ gates
 2. Start with X gate (i.e. $\Pi_{0,1}$ gate)
 3. Apply $\Pi_{1,2}$ and $\Pi_{2,3}$ gates sequentially to raise the energy level
- Gate for going from $|0\rangle$ to $|3\rangle$ energy level:



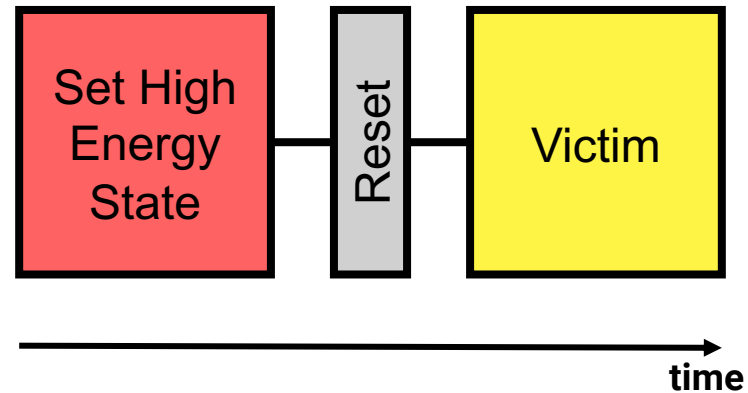
Review of Quantum Computer Workflow

- User's code is transpiled into gate-level code and eventually scheduled as control pulses sent to the quantum computer
- The pulse-level circuits are scheduled on the quantum computer
 - Each circuit execution is called a 'shot'



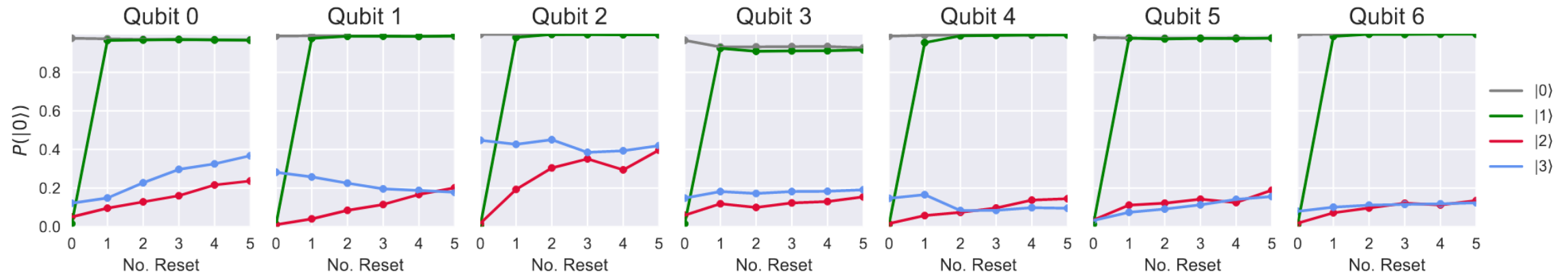
Threat Model

- Attacker scheduled before victim, shot by shot, on the same qubit
- Set qubit state to high energy
- Let victim execute after reset



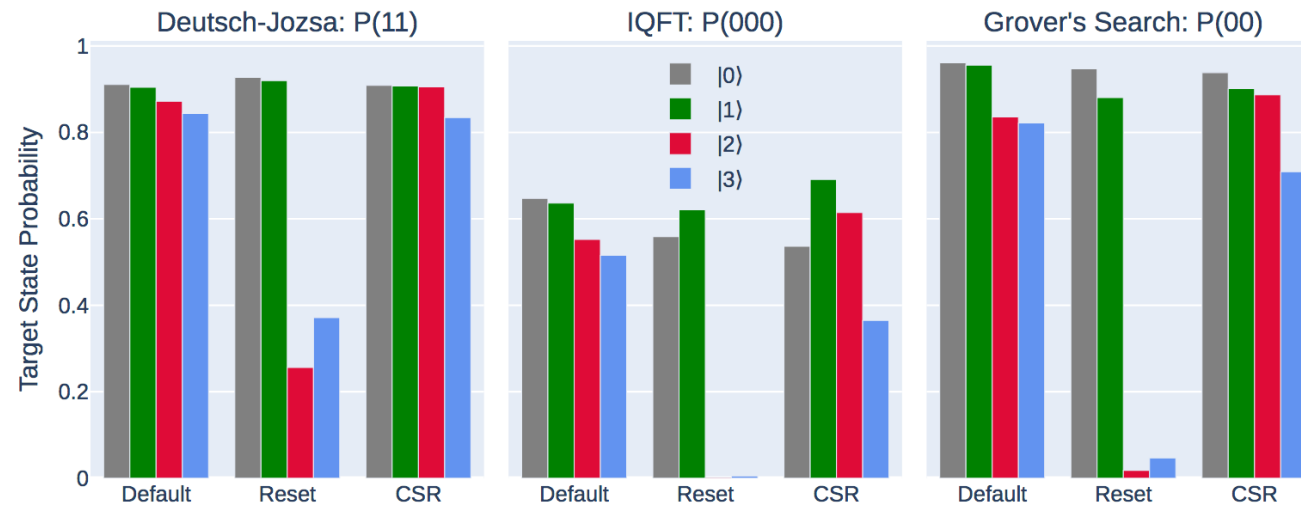
Impact of Higher Energy States

- Basic gates are only calibrated considering two-level system, they do not have the expected effect on higher energy states
- Example of effect on reset gate**
 - Probability of measuring $|0\rangle$ after different number of reset gates
 - Reset is not effective against $|2\rangle$ and $|3\rangle$ states



Impact of Higher Energy States

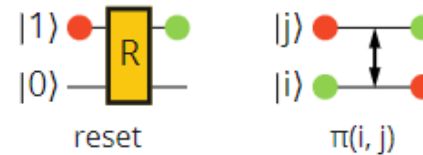
- Higher energy states affect all gates, and circuits made of these gates
- **Example of effect on results of different algorithms**
 - Deutsch-Jozsa
 - Inverse quantum Fourier transformation
 - Grover's search



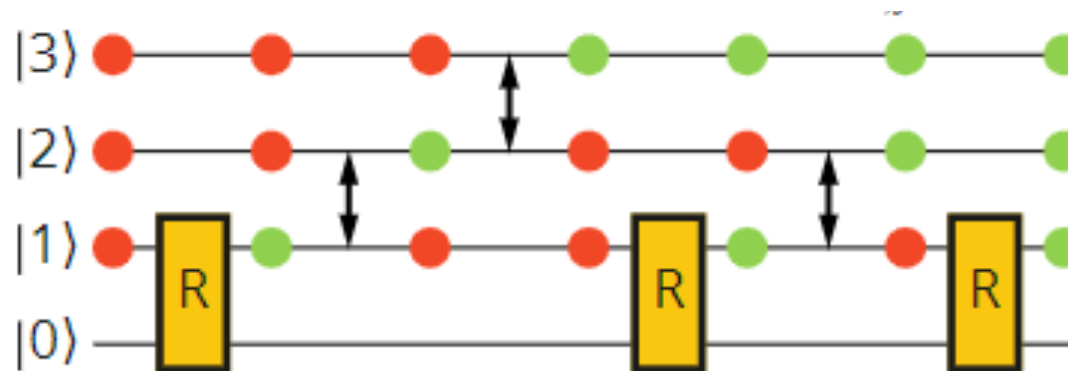
Design of Cascading Secure Reset (CSR) Gate

- Basic idea: sequentially bring down high energy states to lower energy states, down to $|1\rangle$ which can be eliminated using the native reset gate

- Building blocks: reset and Π gates



- Cascading Secure Reset (CSR):



Tutorial Outline

- 1:00pm – 1:30pm: Introduction and Motivation
- 1:30pm – 2:30pm: Crosstalk and Fault Injection in NISQ Quantum Computers
 - Crosstalk and Fault Injection Among Qubits
 - Fault Injection in Reset Gates
- 2:30pm – 3:00pm: Coffee Break
- 3:00pm – 3:45pm: Side Channels in NISQ and FTQC Quantum Computers
- 3:45pm to 4:30pm: Trusted Execution Environments for Quantum Computers
- 4:00pm: End

