CROSSTALK-INDUCED SIDE CHANNEL THREATS IN MULTI-TENANT NISQ COMPUTERS

Navnil Choudhury†, Chaithanya Naik Mude, Preetham Chanda Tikkireddi* ,*
Sanjay Das†, Swamit Tannu and Kanad Basu†*

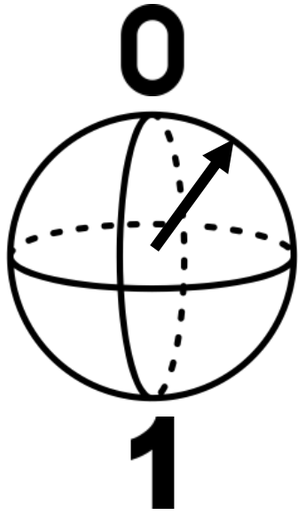
†University of Texas at Dallas,
*University of Wisconsin-Madison

State of Quantum Bits

0

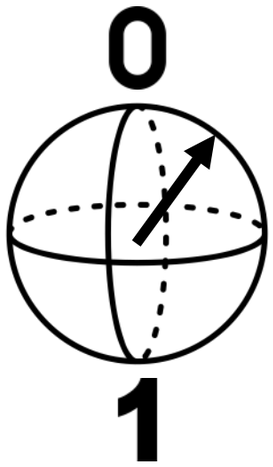
1

Classical bits.

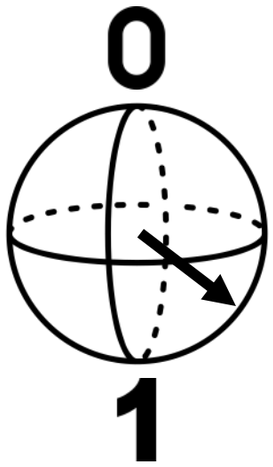


Quantum bits.

A qubit state is a vector that can be visualized as a point on a sphere



Quantum gate



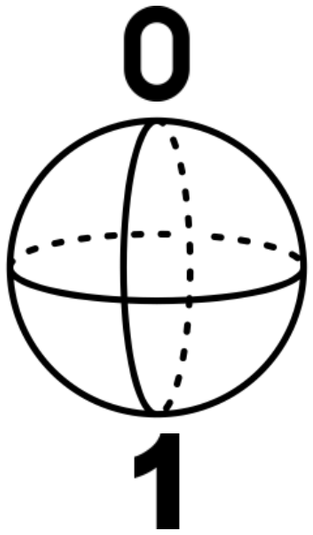
Quantum Gate rotates this vector to manipulate the qubit state

Quantum Computing Basics

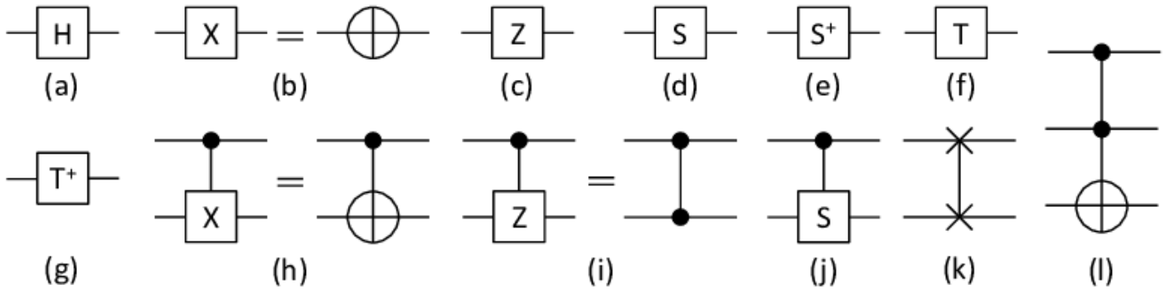
0

1

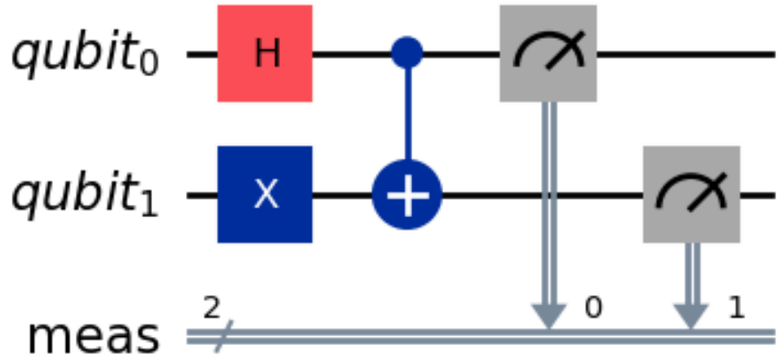
Classical bits.



Quantum bits.



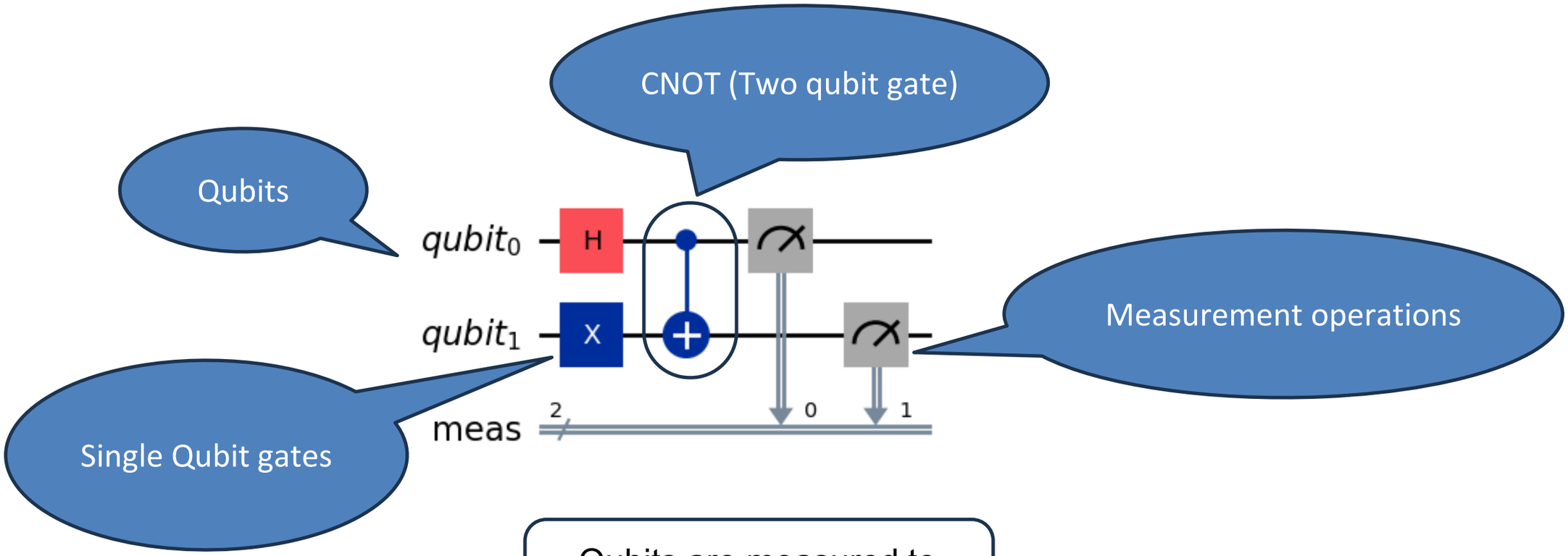
Quantum gates.



Qubits and quantum gates comprise quantum circuits.

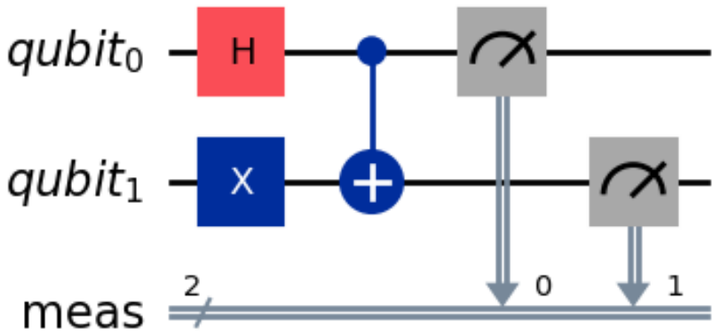
Quantum circuit.

Quantum Computing Basics

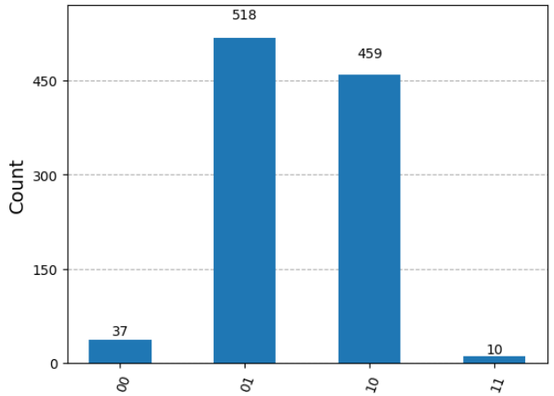


Qubits are measured to provide the final output.

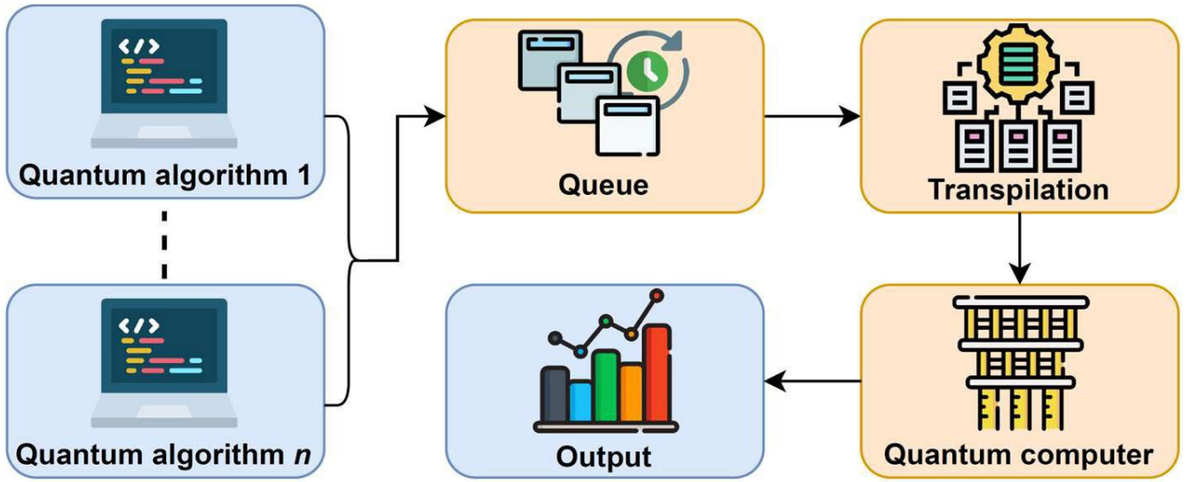
Quantum Cloud



Quantum circuit.

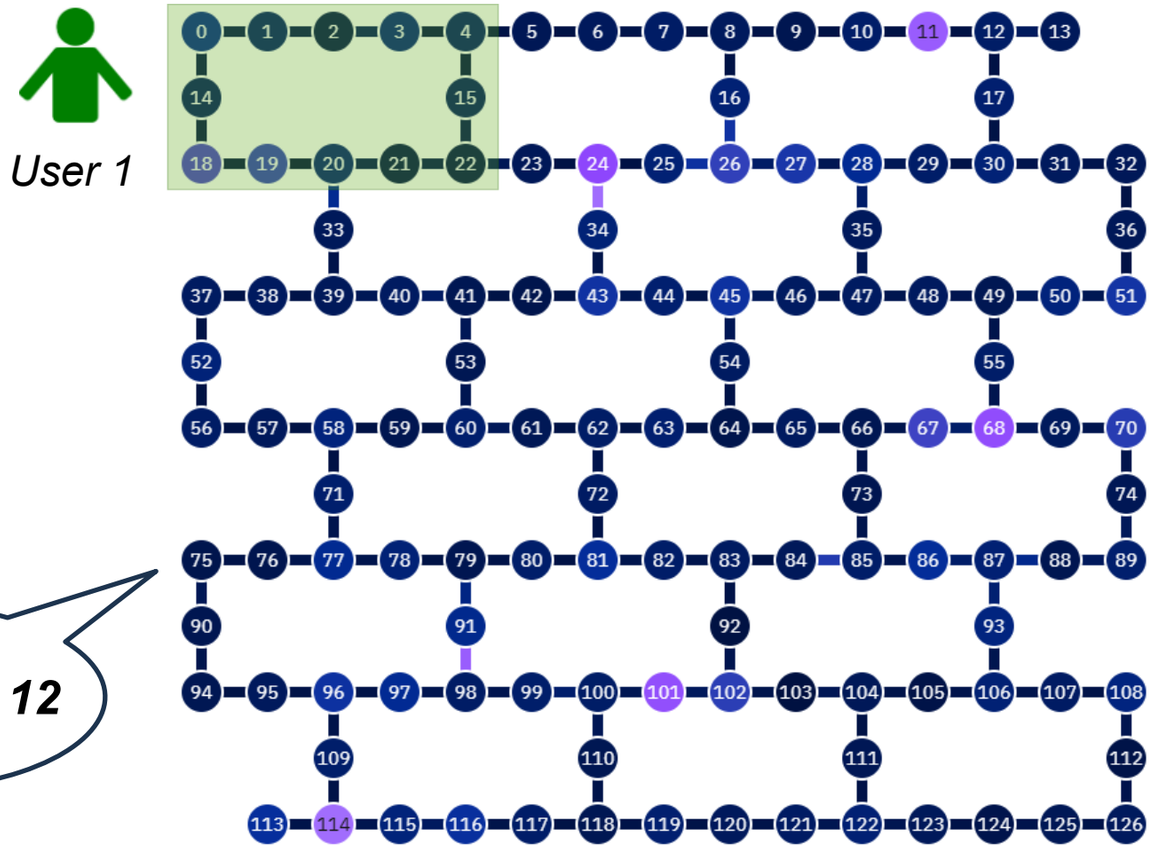


Execution outcomes.



Outline of quantum cloud pipeline.

Why do we need multi-tenancy ?

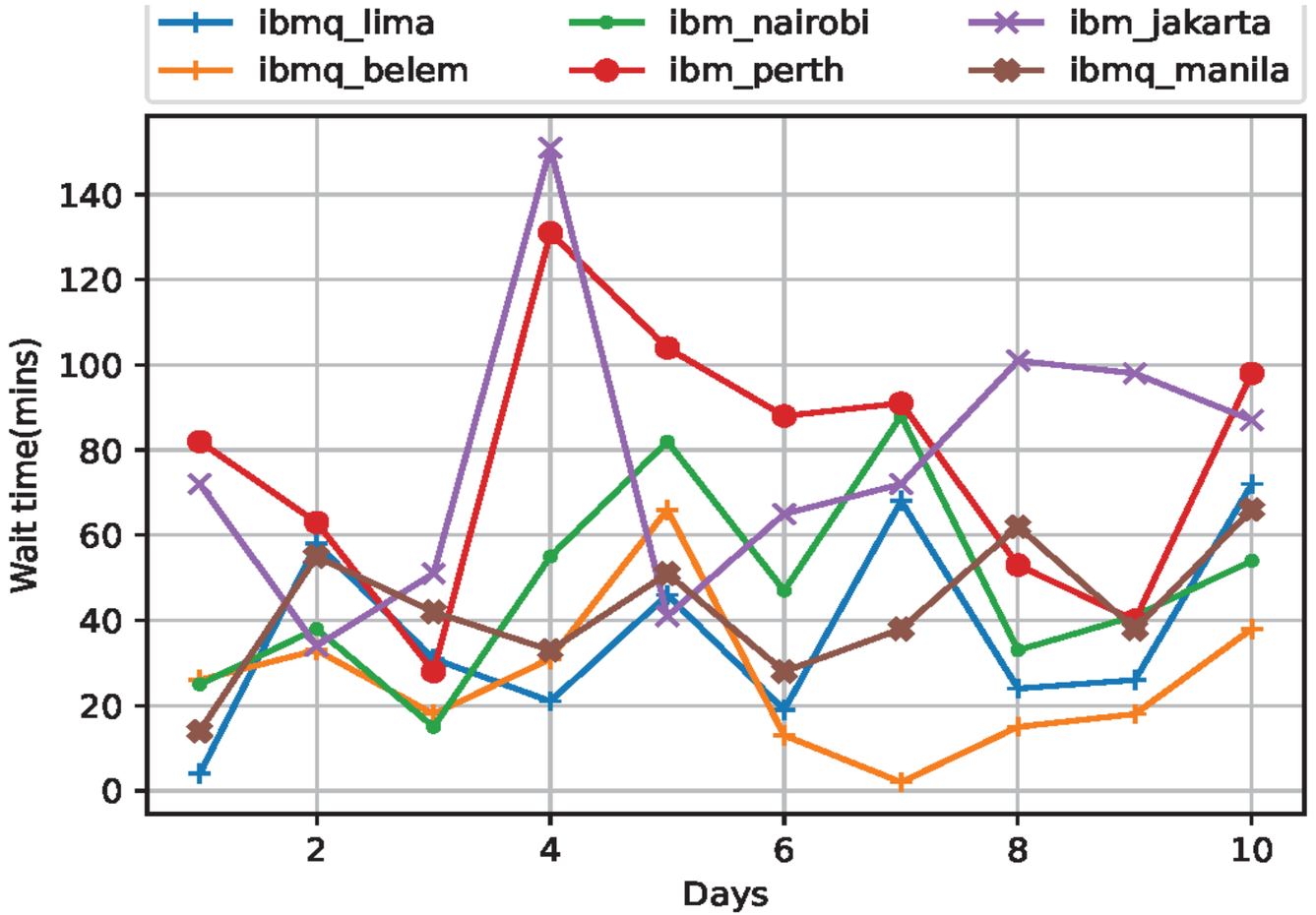


Unused qubits: ***115***

Qubits used: ***12***

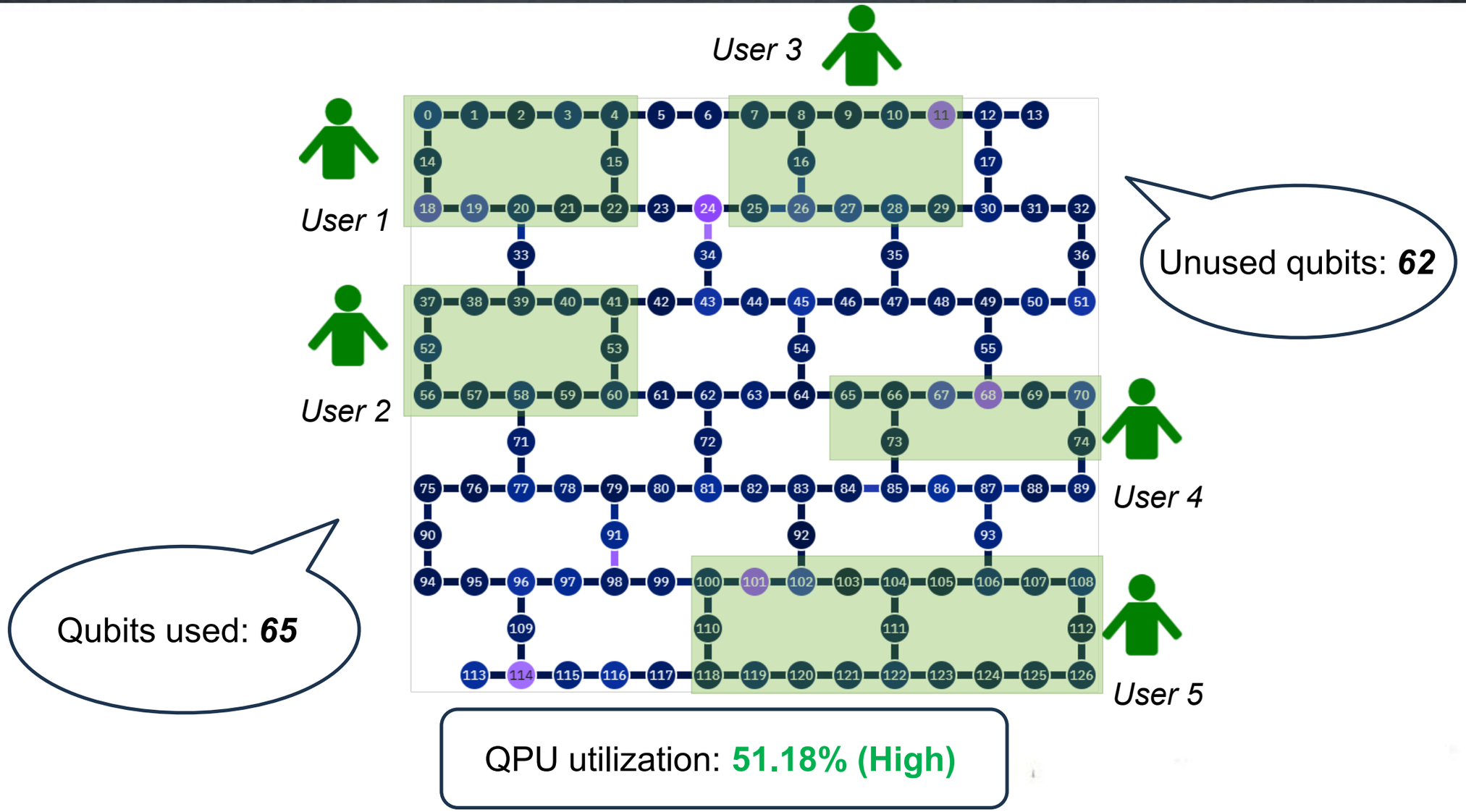
QPU utilization: **9.44% (Very low !)**

Why do we need multi-tenancy ?

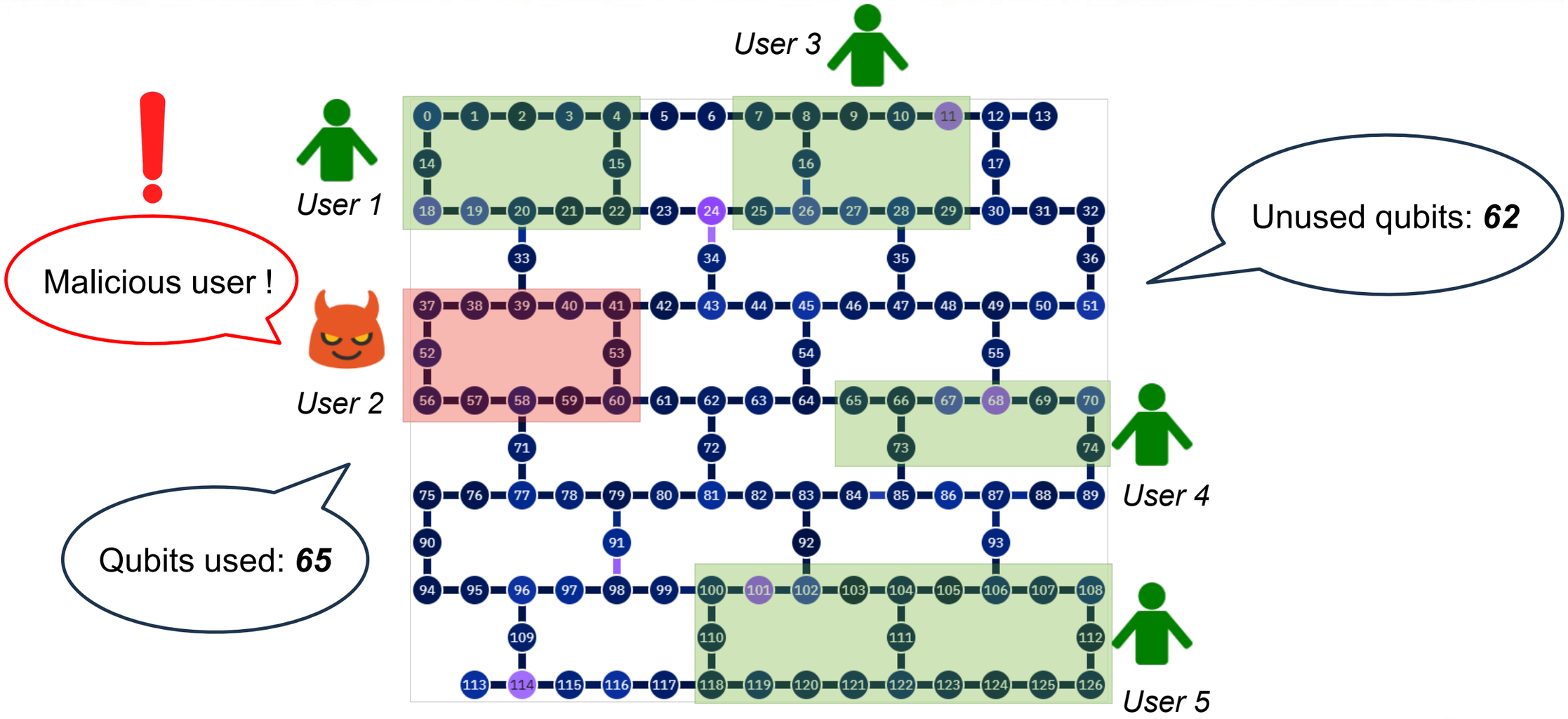


Workload on open-access IBMQ backends over a 10-day period.

Why do we need multi-tenancy ?



Security challenge in multi-tenancy



Why do we care about attacks ?

The Next Breakthrough In Artificial Intelligence: How Quantum AI Will Reshape Our World

Toward a code-breaking quantum computer

Building on a landmark algorithm, researchers propose a way to make a smaller and more noise-tolerant quantum factoring circuit for cryptography.

Adam Zewe | MIT News
August 23, 2024

nature reviews physics

Review article

Check for updates

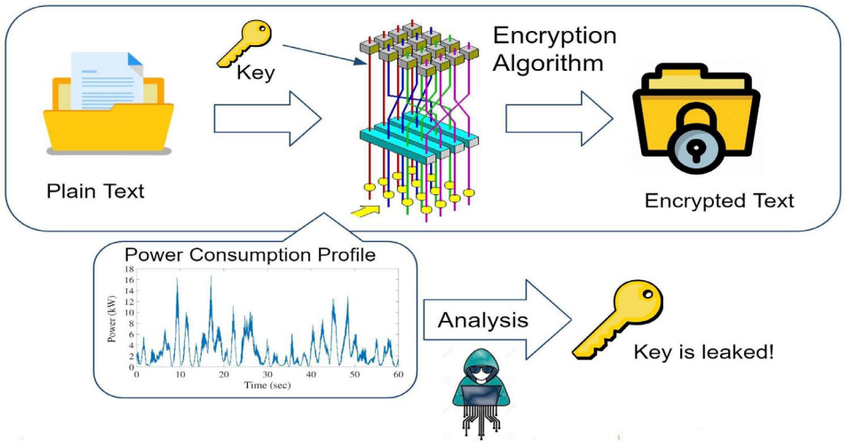
Quantum computing for finance

Quantum is coming — and bringing new cybersecurity threats with it

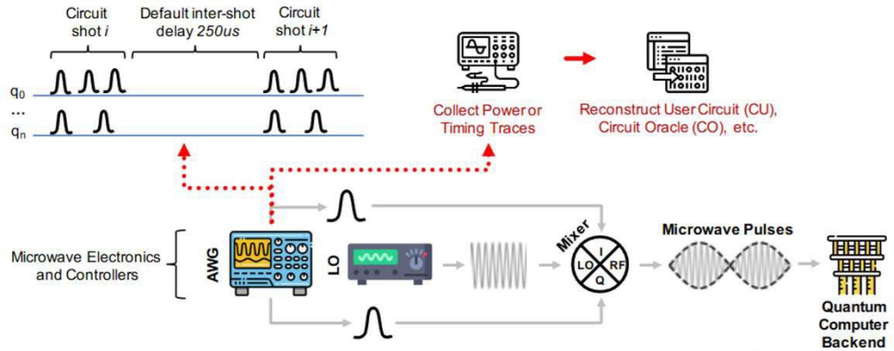
Quantum computing changing the security infrastructure of the digital economy

Side-channel attacks

- Side-channel attacks exploit indirect information leaks.
- Leak sensitive and proprietary data, jeopardizing user information.



Power side-channel attacks[1].

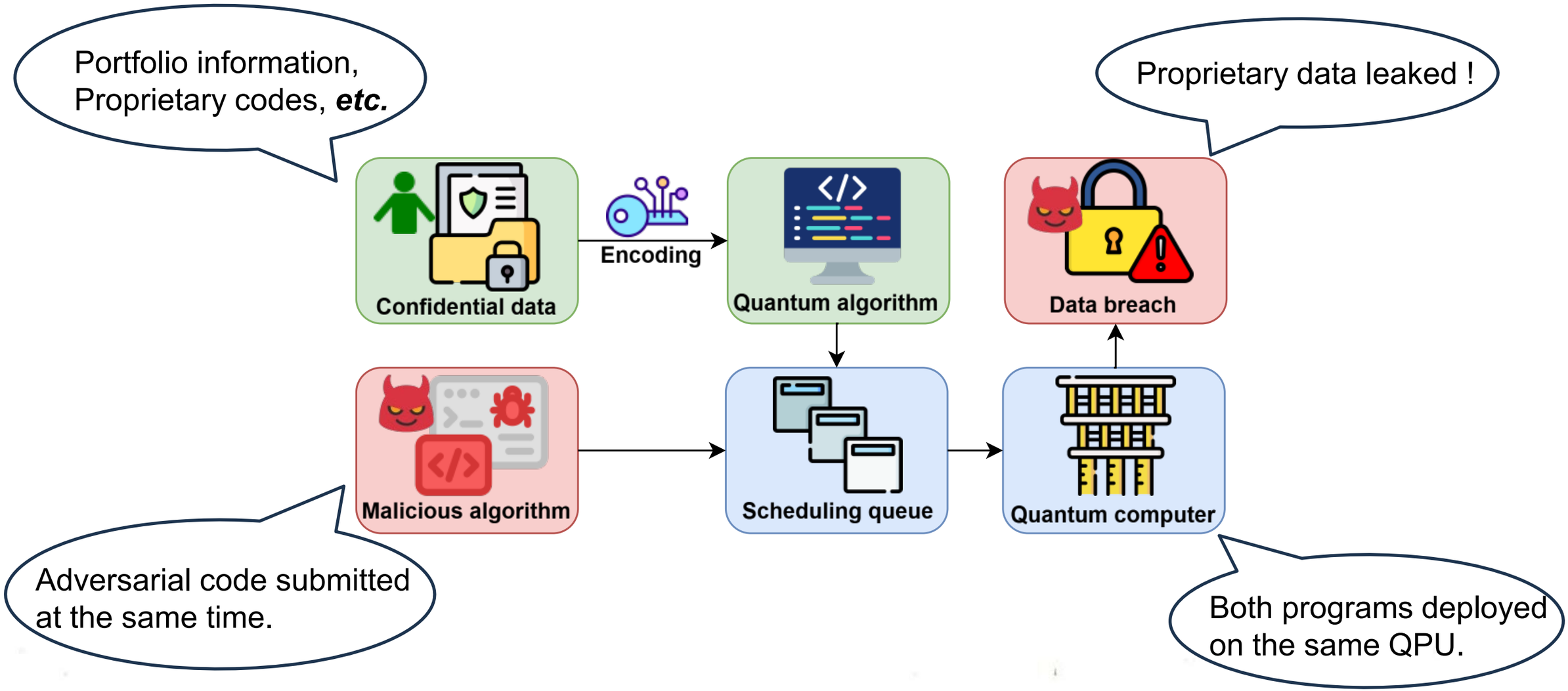


Power side-channel attacks on quantum computers[2].

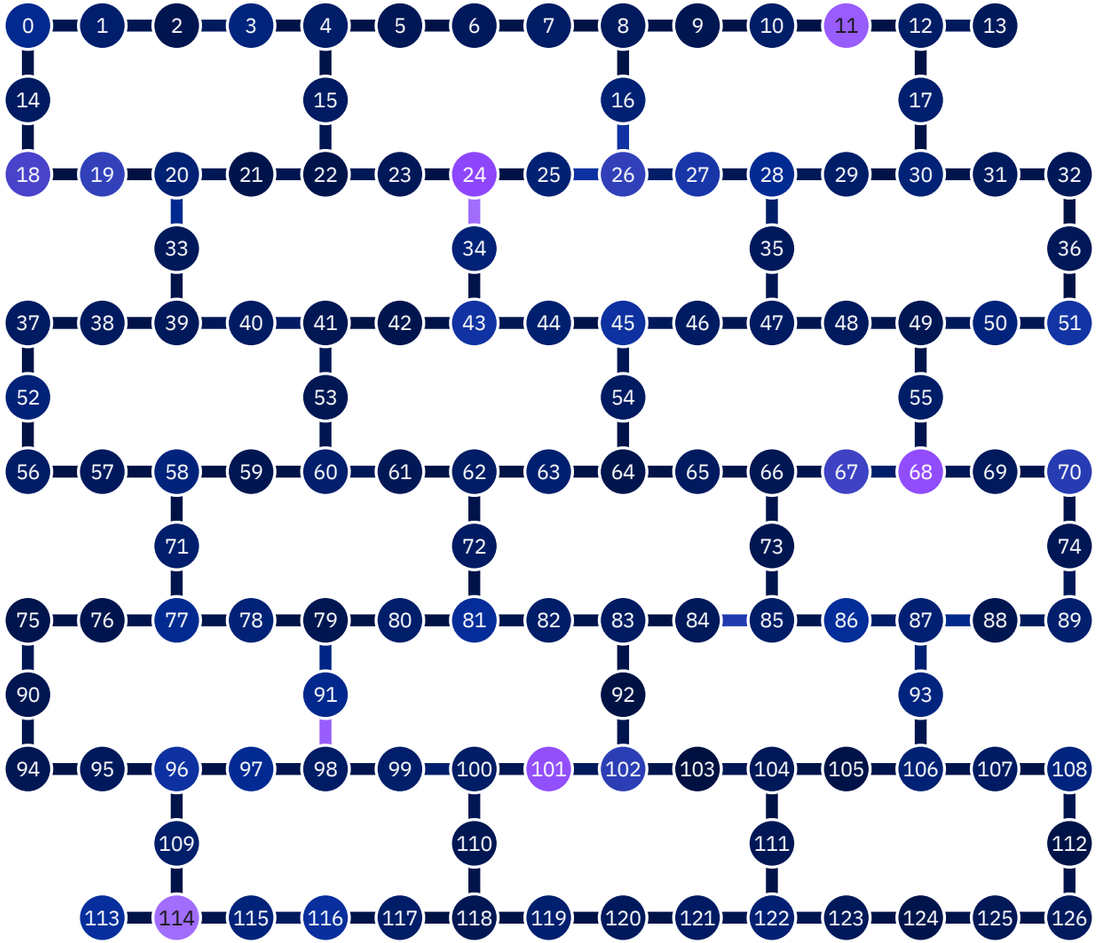
[1]A. Srivastava et al., "SCAR: Power Side-Channel Analysis at RTL Level" in TVLSI Systems, June 2024, doi: 10.1109/TVLSI.2024.3390601.

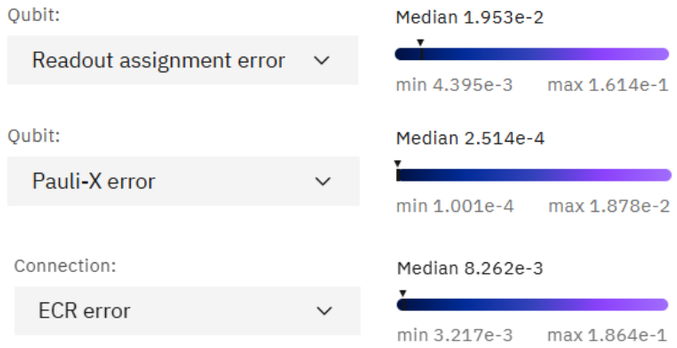
[2]C. Xu, et al., “Exploration of Power Side-Channel Vulnerabilities in Quantum Computer Controllers” in CCS 2023, https://doi.org/10.1145/3576915.3623118.

Quantum side-channels are a new threat !



Errors In Quantum Computers

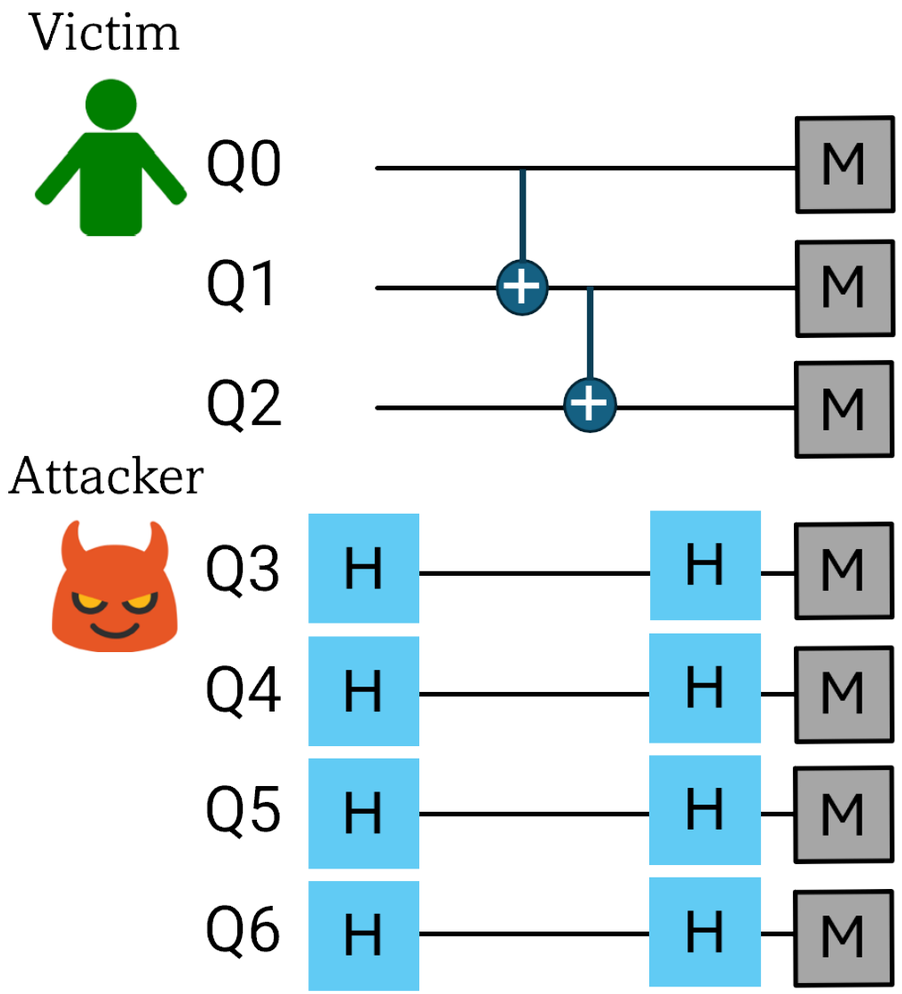




Errors pave the way for attackers to threaten security !

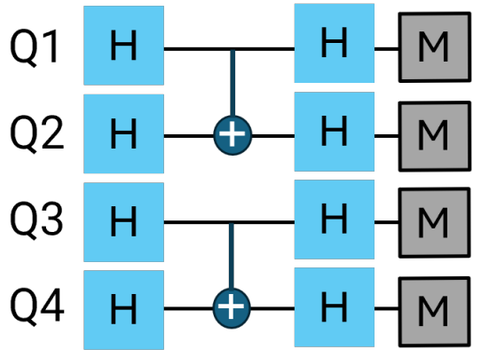
Threat Model Using Crosstalk

- Victim and attacker share a common QPU.
- Victim and attacker can run programs concurrently.
- Attacker is aware of a limited set of useful quantum algorithms.

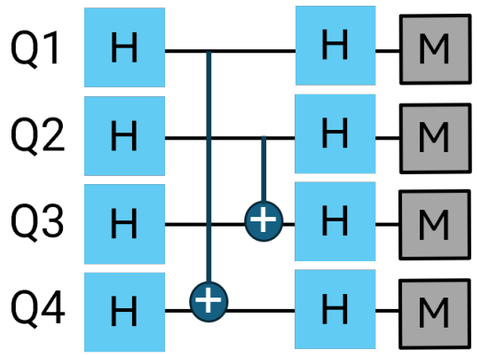


Crosstalk As a Side-Channel

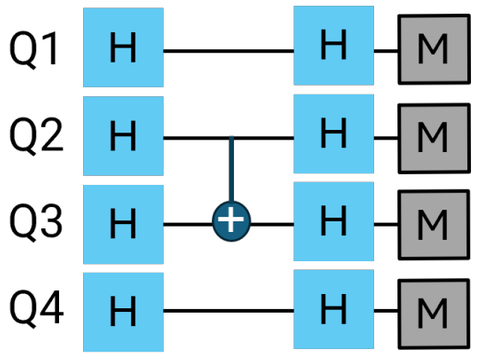
Circuit- a

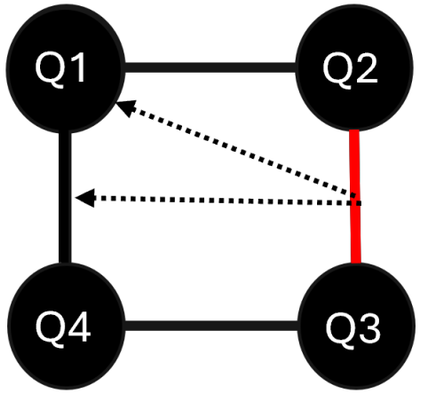


Circuit- b



Circuit- c

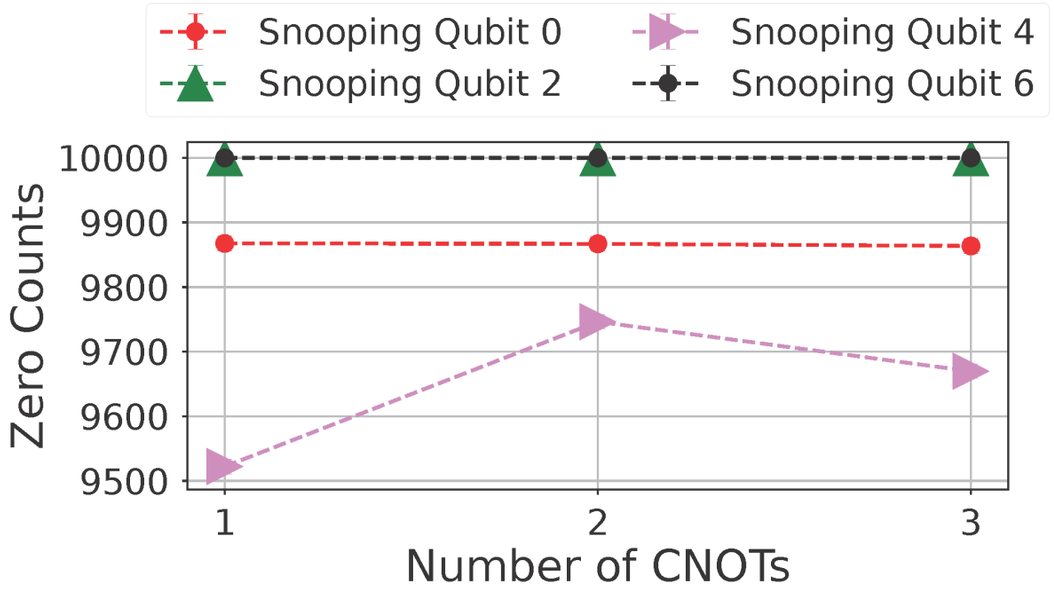




Circuit	Zero Count	Non-Zero Count
a	97	3
b	73	27
c	82	18

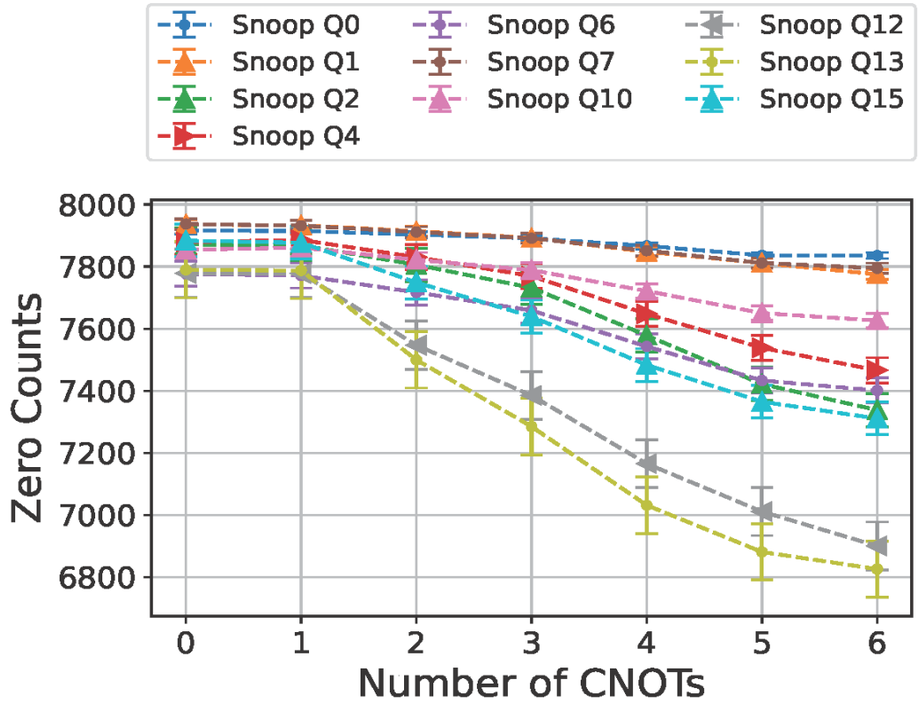
Variations due to crosstalk !

Crosstalk As a Side-Channel

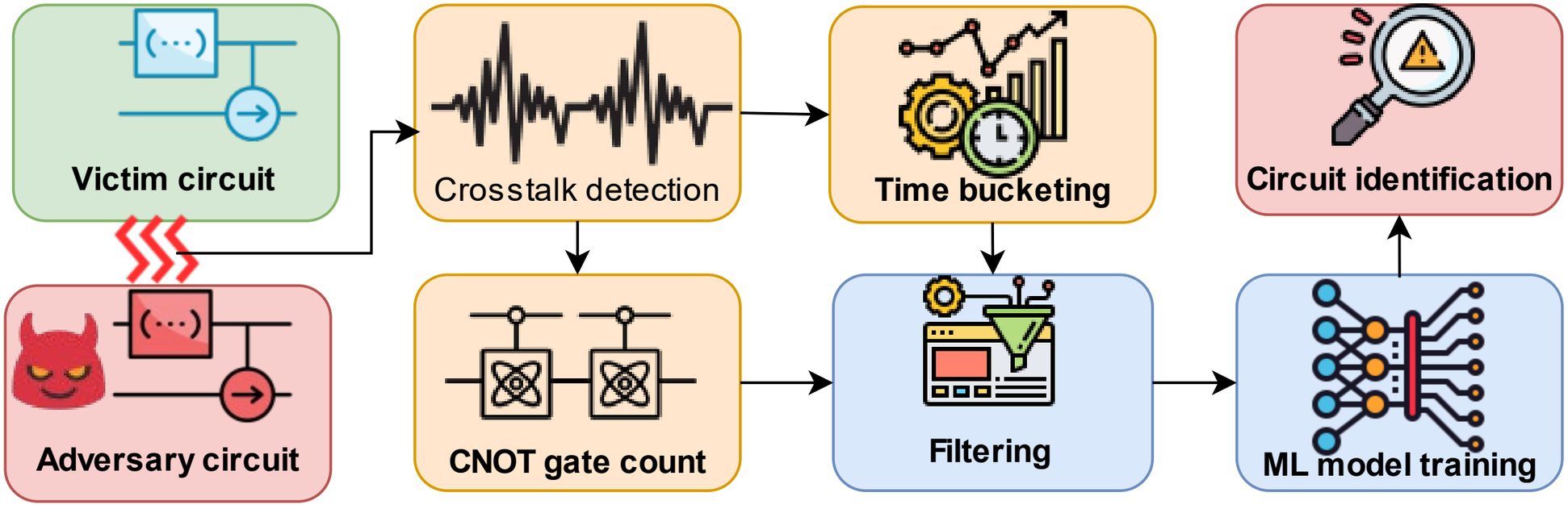


Zero-counts differ based on snooping qubit used.

Scalability of CNOT gate counting depends on snooping qubit.

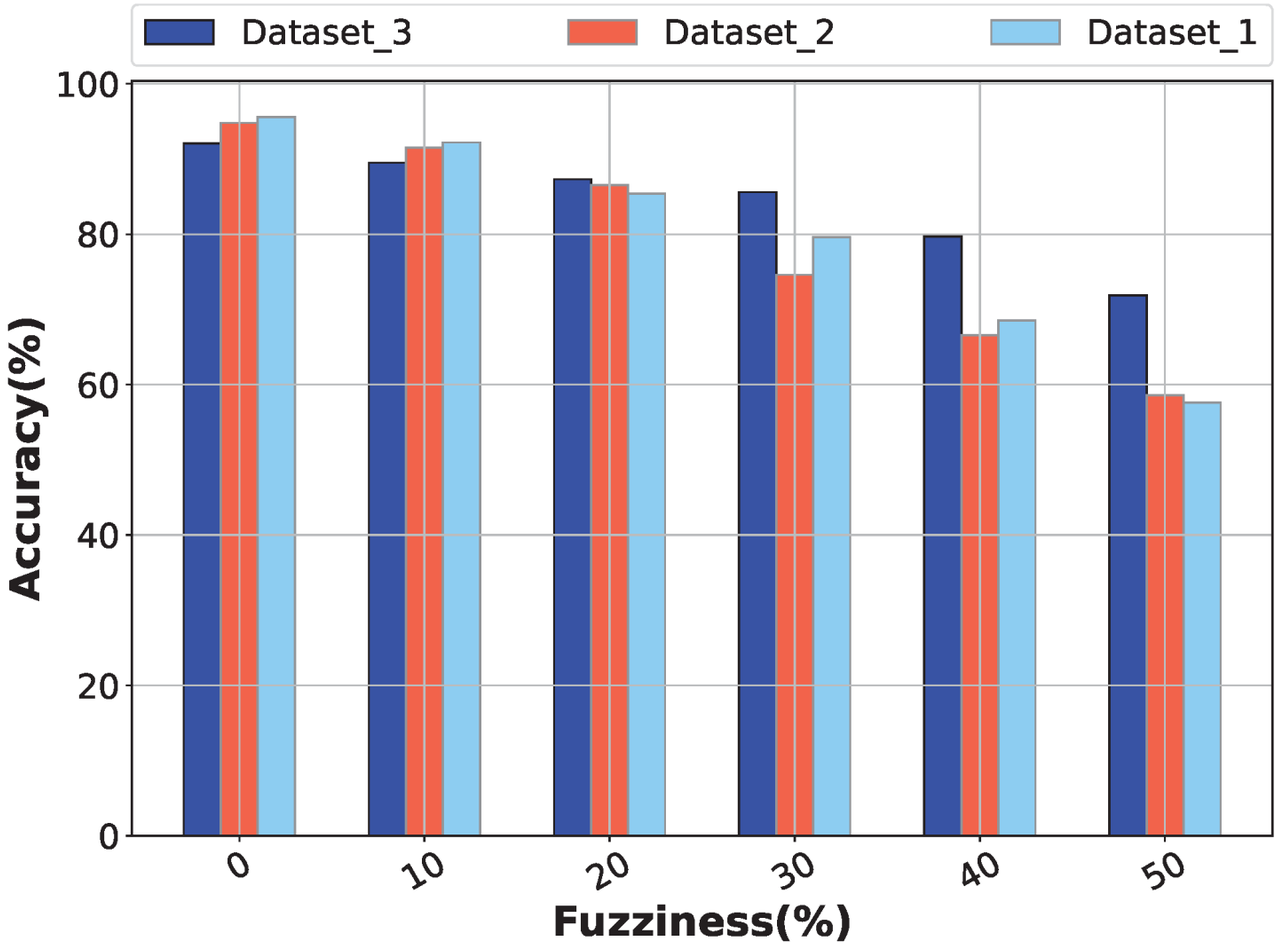


Proposed attack



Overview of the proposed attack.

Results



Fuzziness denotes erroneous data received during crosstalk detection.

Conclusion

- The paper shows a quantum side-channel attack exploiting crosstalk in NISQ systems.
- The paper focuses on exposing vulnerabilities in shared multi-tenant computing.
- The threat model was evaluated using adversarial qubits under realistic constraints.
- The relevance of CNOT gates in quantum circuit identification was demonstrated.
- The trained GCN-based model, achieving 85.6% accuracy in identifying victim circuits.
- Potential defense strategies were discussed against quantum side-channel attacks.
- This research emphasizes the need for security in collaborative quantum computing.

THANK YOU

CROSSTALK-INDUCED SIDE CHANNEL THREATS IN MULTI-TENANT NISQ COMPUTERS

Navnil Choudhury

Chaithanya Naik Mude

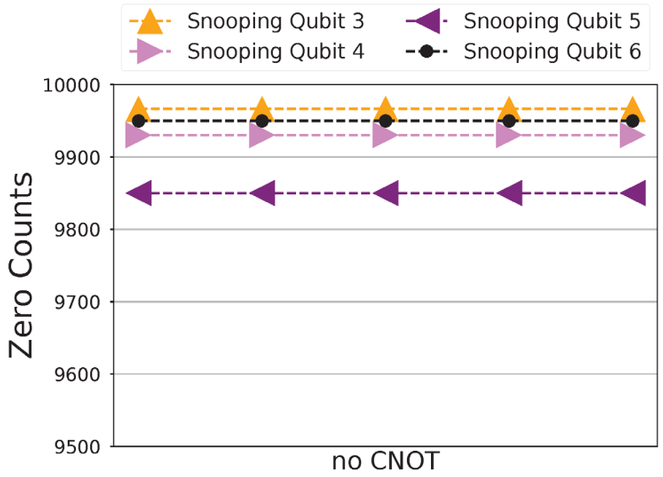
Preetham Chandra Tikkireddi

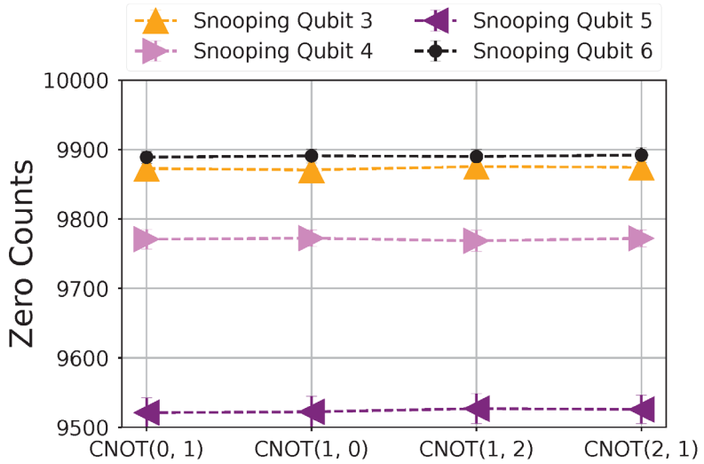
Sanjay Das

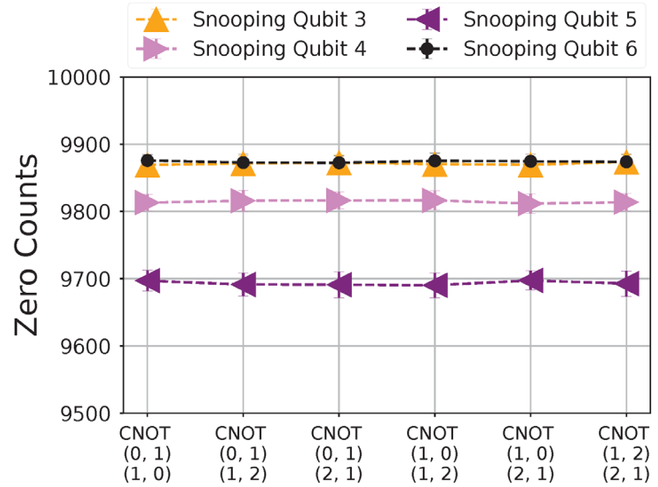
Dr. Swamit Tannu

Dr. Kanad Basu

Crosstalk Gate Detector



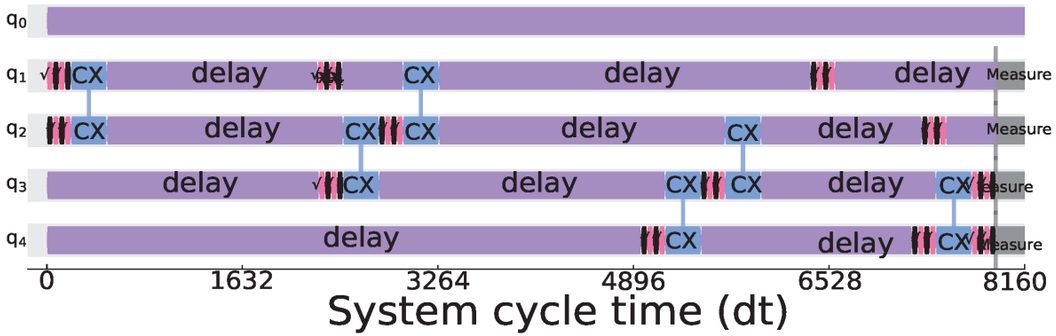




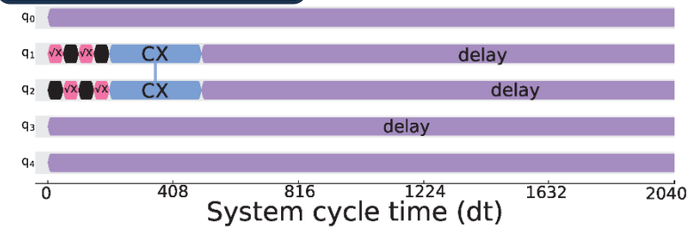
Changes in zero counts due to crosstalk correlate to the number of CNOT gates.

Time bucketing of CNOT data

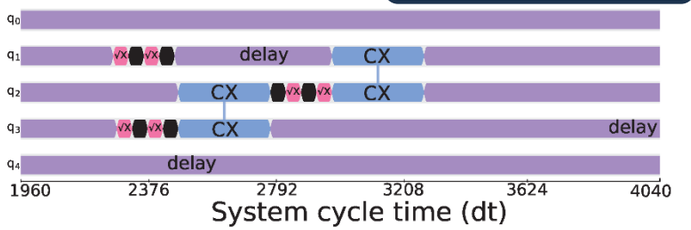
Timing diagram captures temporal distribution of CNOT gates during execution.



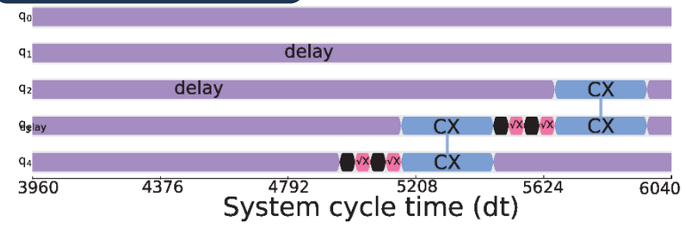
Time bucket 1



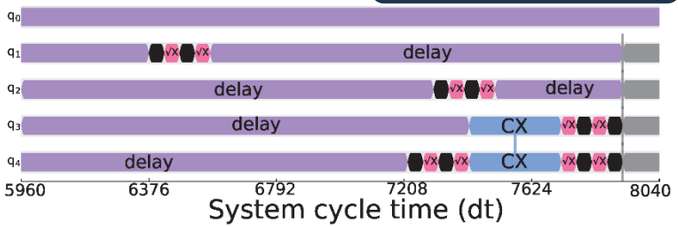
Time bucket 2



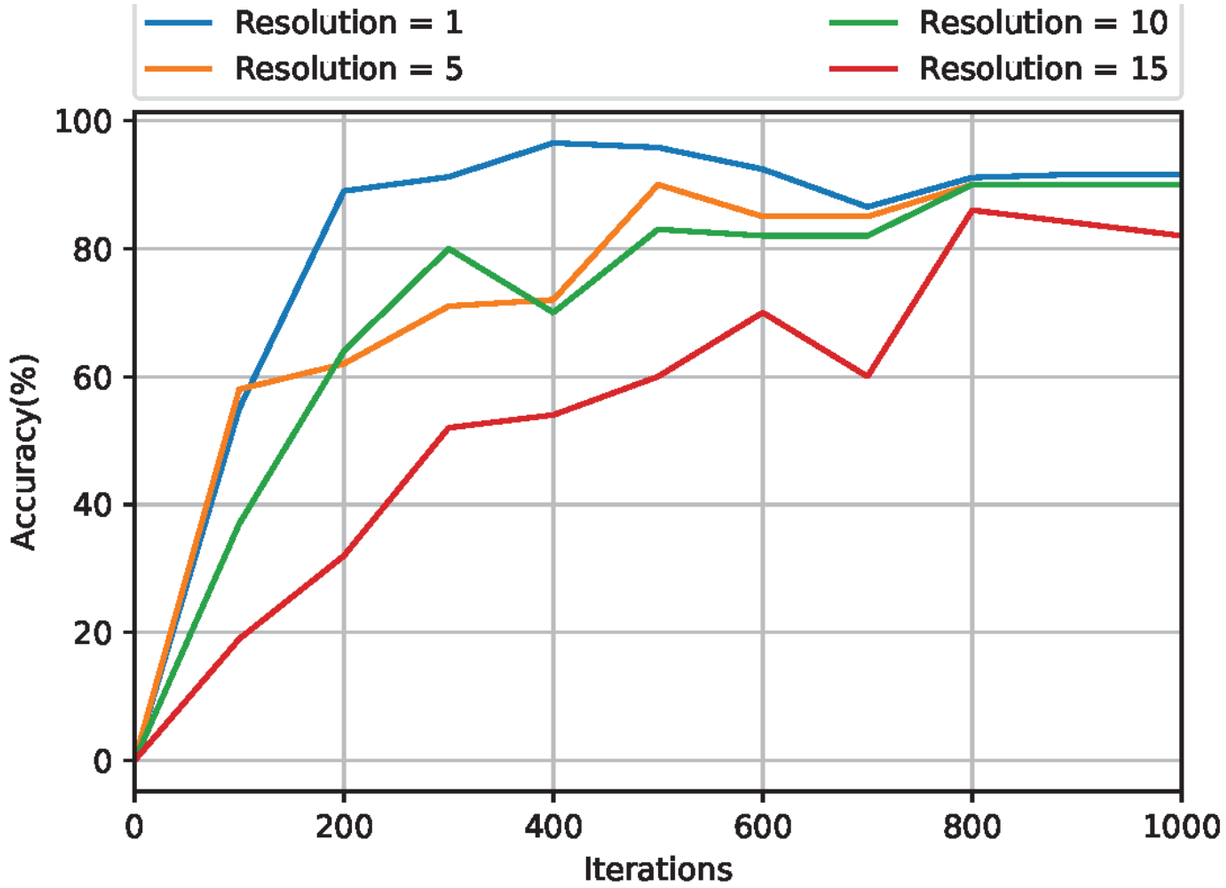
Time bucket 3



Time bucket 4



Resolution



Resolution denotes duration of timing bucket during dataset creation.