# QubitVise: Double-Sided Crosstalk Attack in Superconducting Quantum Computers

Adriana Aranguren Arellano[†]
Northwestern University
Evanston, IL, USA
adrianaarangurenarellano2025@u.northwestern.edu

He Xie[†]
Northwestern University
Evanston, IL, USA
hexie2026@u.northwestern.edu

Jakub Szefer
Northwestern University
Evanston, IL, USA
jakub.szefer@northwestern.edu

***Abstract*—This work presents a novel security attack based on $CNOT$ gate induced crosstalk in superconducting qubit systems. Compared to previous work, this work introduces a double-sided crosstalk attack where attacker's circuits are located on either side of the victim circuit executing in a multi-tenant cloud-based quantum computer. The attacker, a malicious tenant or user, can interfere with, or disrupt, the state of neighboring qubits in the victim tenant or user without direct access to victim's qubits, by taking advantage of interference and crosstalk among the otherwise logically isolated qubits. New aspect of this attack is the location of the attacker's circuits on both sides of the victim. Experimental validation on cloud-based Rigetti quantum devices demonstrates that these attacks can compromise data integrity and cause the victim's circuit's outputs to change. Magnitude of the change is evaluated using total variational distance and tested on number of common benchmarks that can execute on today's quantum computers. This work underscores the need for improved isolation mechanisms and secure scheduling in multi-tenant quantum computing cloud environments.**

***Index Terms*—quantum computing, security attacks, crosstalk**

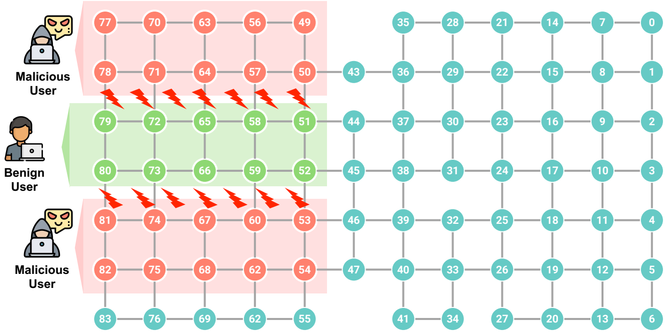


Fig. 1: Overview of the QubitVise attack: attacker's malicious circuits on two sides of the victim induce crosstalk noise in the victim to interfere with the victim's computation. Example attacker and victim locations are overlaid on top of the Rigetti Ankaa-3 quantum computer topology.

## I. Introduction

In today's Noisy Intermediate-Scale Quantum (NISQ) era, access to quantum hardware is increasingly facilitated through cloud-based platforms. Major technology providers such as IBM Quantum [1], Amazon Braket [2], Microsoft Azure Quantum [3], and Rigetti Computing [4] offer remote access to their Quantum Processing Units (QPUs). Google is also actively investing in quantum computing through its Google Quantum AI initiative [5], with plans to establish its own cloud-based quantum hosting infrastructure. In these environments, QPUs are shared resources, time-multiplexed among multiple users. Clients submit quantum algorithms for execution on real quantum hardware, after which the QPU is reallocated to serve other users.

### A. Motivation

As quantum hardware remains scarce and expensive, cloud-based quantum computing platforms can increase their utilization through a multi-tenant model. In such setting, multiple users share access to the same QPU, executing jobs in parallel on the same QPU. Although not currently available from major quantum computer providers, multi-tenant QPUs have been actively explored in research [6]. The functional and economic benefits of multi-tenant quantum computers could be, however impacted by new types of security issues that such deployments face. The focus of this work is to help better understand the potential security threats in multi-tenant quantum computers.

The security analysis is further motivated by the potentially valuable data and algorithms that will execute on quantum computers. Although the practical adoption of quantum computing remains in its early stages, its integration with artificial intelligence (AI) is anticipated to transform critical domains such as finance, pharmaceuticals, and cryptography. For example, several pharmaceutical companies are leveraging quantum computers to simulate molecular behavior with greater speed and accuracy, aiming to accelerate drug discovery and reduce adverse side effects. However, utilizing the quantum hardware necessitates reliance on the remote cloud providers, introducing need for trust and security issues to be evaluated.

### B. QubitVise Overview

Figure 1 shows the overview of the QubitVise attack. In the attack, the attacker's malicious circuits on two sides of the victim induces crosstalk noise in the victim to interfere with the victim's computation. Example attacker and victim

[†] Students, listed in alphabetical order, contributed to early evaluation of the ideas presented in this paper as part of the Secure Quantum Computing course at Northwestern University.

[‡] This work was supported in part by NSF grant 2332406.

locations in the figure are overlaid on top of the Rigetti Ankaa-3 quantum computer topology on which the attacks from this work have been evaluated.

Unlike prior crosstalk attacks which have considered only one attacker circuit typically on one side of the victim [7], [8], this work focuses on using two attacker circuits. Recent work [9] has evaluated having aggressor qubits on two sides of a single qubit in IBM quantum computers, however, it did not test actual quantum circuits under the crosstalk attack from two sides of the victim.

### C. Results Highlight and Contributions

The evaluation presented later in this paper shows that double-sided crosstalk attack on average causes the total variational distance to increase 13% compared to only one sided attack. The maximum increase was 35%. Further, in some tests the increase was up to 223%, however, this may be an outlier and was not used in computing the average. The combined data indicates that the presented attack can be used to increase the effectiveness of the prior crosstalk attacks in a significant way. The evaluation code is available online at https://github.com/caslab-code/qc-qubit-vise.

## II. Threat Model

This work considers a minimal threat model in which a malicious user possesses only standard, user-level access to a quantum computing platform and can execute basic two-qubit gates such as $CNOT$. These capabilities are currently available in all gate-based quantum computing platforms such as IBM, Rigetti, and IQM. We assume the adversary can locally compile quantum circuits and ensure the circuit contains many $CNOT$ gates, before submitting it to the quantum backend. Our assumption implies that the compiler nor cloud provider can detect nor eliminate circuits that have many $CNOT$ gates. Prior work on quantum computer antivirus showed, for example, that adding delays between $CNOT$ gates prevents compiler from optimizing them away [7]. Recent work showed that QAOA-type circuits contain my $CNOT$ gates and crosstalk attacks can be disguised as QAOA-type circuits making their detection difficult [10]. As we are considering a multi-tenant setting, we assume that the attacker is able to co-located with the victim on the same quantum computer and to allocate qubits that are physically on either side of the victim, as shown in Figure 1.

## III. Evaluation Setup

In this work we evaluate the new attack on a set of common quantum circuits. We use 2-qubit Bell State circuit, 4-qubit Ising circuit, and 6-qubit GHZ State circuit as the victim circuits. These circuits are commonly found as part of benchmark suits such as QASMBench [11]. We evaluate the attacks on Rigetti Ankaa-3 quantum computer available for cloud-based access from Amazon Braket. For the attacker circuits, we use simple circuits with many $CNOT$ gates.

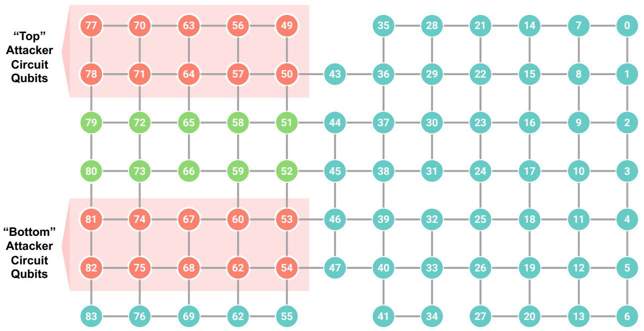

"Top" Attacker Circuit Qubits
"Bottom" Attacker Circuit Qubits

Fig. 2: Location of the attacker circuits in the Rigetti Ankaa-3 quantum computer.

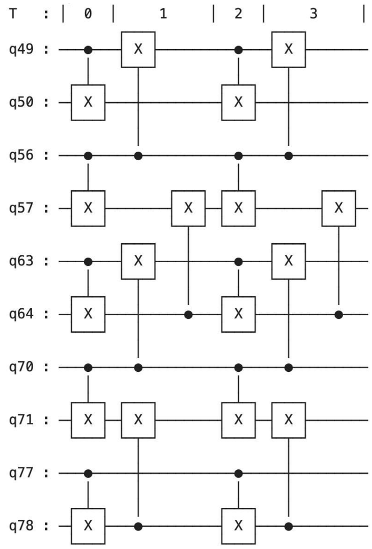


Fig. 3: Example schematic of attacker "top" circuit.

### A. Quantum Computer Setup

The attacks are evaluated on Rigetti Ankaa-3 quantum computer available for cloud-based access from Amazon Braket [2]. The testing was done trough qBraid quantum computing environment from which jobs were submitted to Amazon Braket. Python-based Braket programming environment was used to write and submit circuits for execution on Ankaa-3.

### B. Attacker Circuits and their Placement

The attacker circuits are simple circuits composed of $CNOT$ gates. The attacker circuits use 10 qubits. We use two attacker circuits on qubits $77, 78, 70, 71, 63, 64, 56, 57, 49, 50$ ("top" attacker circuit) and on qubits $81, 82, 74, 75, 67, 68, 60, 62, 53, 54$ ("bottom" attacker circuit in the Rigetti Ankaa-3 quantum computer. Figure 2 shows the location of the attacker circuit qubits. The attacker circuits use only 18 $CNOT$ gates in total, the depth of the attacker circuit is only 4; sample attacker circuit is shown in Figure 3.

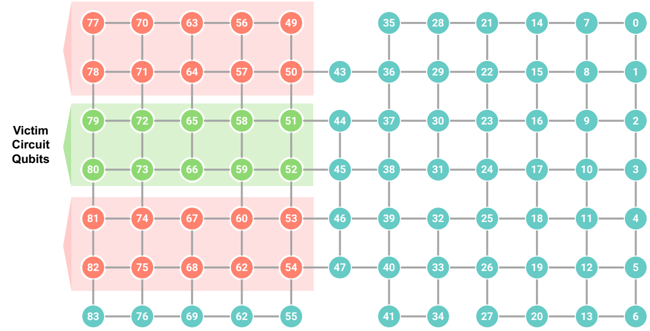


Fig. 4: Location of the victim circuits in the Rigetti Ankaa-3 quantum computer.

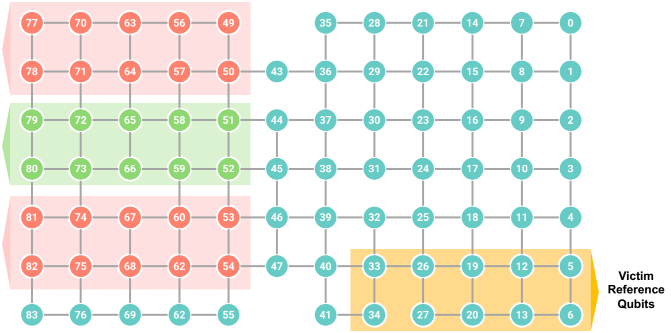


Fig. 5: Location of the victim reference circuits in the Rigetti Ankaa-3 quantum computer.

### C. Victim Circuits and their Placement

The victim circuits are physically located in-between the attacker circuits. Figure 4 shows the location of the victim circuits. Not all the victim circuits use all the qubits. We use 2-qubit Bell State circuit, 4-qubit Ising circuit, and 6-qubit GHZ State circuit as the victim circuits located on qubits $72, 65$, $79, 80, 73, 72$, and $65, 72, 79, 66, 73, 58$ respectively. The circuit details are below.

The *Bell State circuit* creates a two-qubit maximally entangled state. It begins by applying a Hadamard gate to the first qubit, putting it into an equal superposition of $|0\rangle$ and $|1\rangle$. Next, a $CNOT$ gate is applied, using the first qubit as control and the second as target. The result is the entangled Bell state, which is an equal superposition of $|00\rangle$ and $|11\rangle$.

The *Ising circuit* simulates quantum spin interactions based on a one-dimensional Ising Hamiltonian. This circuit typically alternates between single-qubit $X$-rotation gates and two-qubit $ZZ$ entangling gates that act on neighboring qubits. It models both local magnetic field effects and nearest-neighbor coupling, making it a common structure for quantum simulation tasks and variational algorithms such as VQE.

The *GHZ State circuit* generates a highly entangled multi-qubit state exhibiting global correlations across all qubits. The process starts by applying a Hadamard gate to the first qubit to create a superposition. Then, a series of $CNOT$ gates are applied, each with the first qubit as control and one of the remaining qubits as target. This results in a GHZ state, which is an equal superposition of all qubits being in the $|0\rangle$ state and all being in the $|1\rangle$ state.

### D. Victim Circuit Reference Placement

In order to evaluate the effect of crosstalk we utilize a second copy of each victim circuit placed in a separate location within the quantum computer. In particular, Figure 5 shows the location where reference circuits are placed. To compare the effects of the crosstalk on a victim circuit to behavior of an unaffected victim circuit, we need to execute the same victim circuit in a location that is unaffected by crosstalk. By assigns the reference, i.e. unaffected, victim circuit to qubits in the bottom-right of the Rigetti Ankaa-3 quantum computer it is far away from the qubits where $CNOT$ gates execute, and so the location in the bottom-right should not be impacted by the crosstalk.

## IV. Evaluation Results

In this section we analyze the presented double-sided attack, as well as compare it to single-sided attacks.

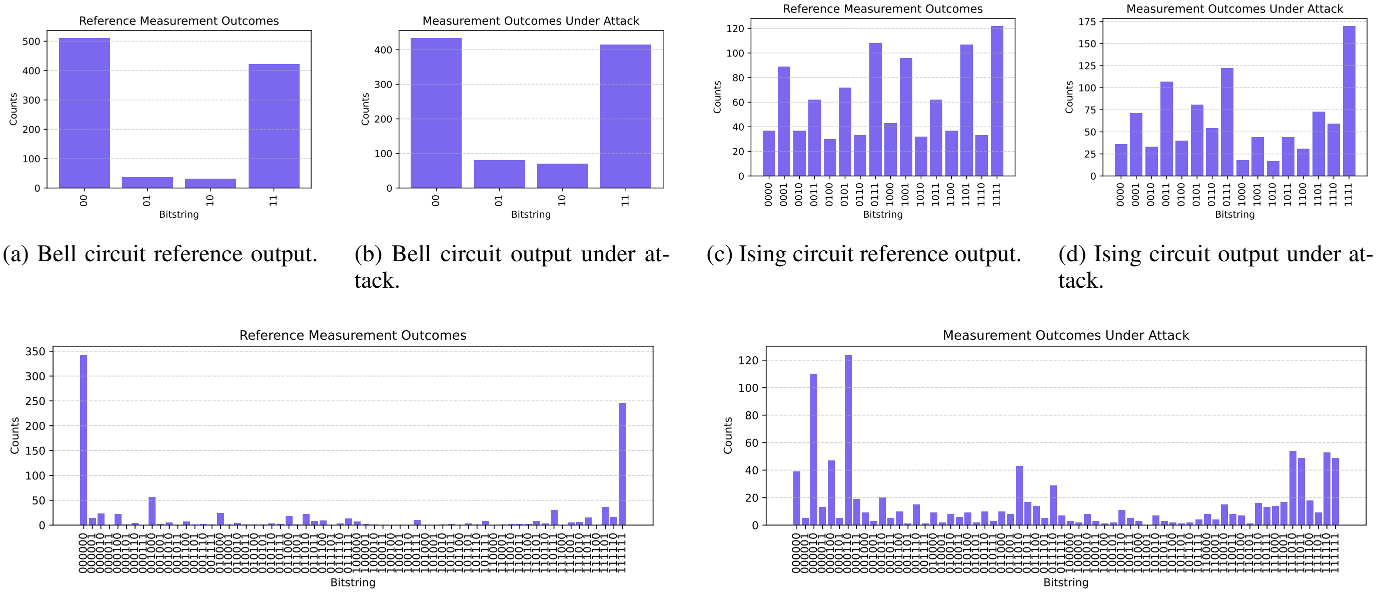
### A. Double-Sided Attack

The results of the evaluation of the new QubitVise double-sided attack are shown in Figure 6. The graphs show the output probabilities for each circuit tested. Reference outputs (when circuit is not under attack) are used to compare to the outputs when the circuit is under attack. The data were collected in June 2025 from the Ankaa-3 quantum computer. Each circuit was executed for 1000 shots to collect the output probabilities for the different states for each circuit.

To quantify the impact of the attack, Table I, shows the total variational distance. Total variation distance is a standard measure of how different two probability distributions are. A distance of zero indicates that the distributions are identical, while a distance of one implies that they are completely disjoint. Here the reference outputs (and probabilities) are used as the baseline, the total variational distance is used to show how different the outputs under attack are from the reference outputs. We can observe the total variational distance to be in the range from 0.026 to 0.653. We observe the TVD in general increases (regardless of the attack type) as the circuit size increases. This may be due to combined effect of some decoherence (larger circuits have more gates and will be impacted more by decoherence), as well as longer time that the attacker has to interfere with the victim.

### B. Single-Sided Attacks

In addition to the double-sided attacks, we tested single sided attacks. In the single-sided attacks, the attacker circuit was simply on “top” of the victim or on the “bottom”. The effective number of $CNOT$ gates in the attacker was half compared to the double-sided attack. The results of the single-sided attacks are quantified in the Table I as well.



(a) Bell circuit reference output.

(b) Bell circuit output under attack.

(c) Ising circuit reference output.

(d) Ising circuit output under attack.

(e) GHZ circuit reference output.

(f) GHZ circuit output under attack.

Fig. 6: Output probabilities for the circuits tested in this work: output without attack (a), (c), and (e); and output under attack (b), (d), and (f).

TABLE I: Total Variation Distance (TVD) of the outputs of the tested victim circuits under single- and double-sided crosstalk attacks.

| Victim Circuit | Attack Type | TVD | Double-Sided TVD Increase |
|---|---|---|---|
| bell, 2 qubit | Double-Sided | 0.084 | – |
| bell, 2 qubit | Single-Sided, Top | 0.026 | 223% |
| bell, 2 qubit | Single-Sided, Bottom | 0.062 | 35% |
| ising, 4 qubit | Double-Sided | 0.173 | – |
| ising, 4 qubit | Single-Sided, Top | 0.153 | 13% |
| ising, 4 qubit | Single-Sided, Bottom | 0.166 | 4% |
| ghz, 6 qubit | Double-Sided | 0.653 | – |
| ghz, 6 qubit | Single-Sided, Top | 0.648 | 1% |
| ghz, 6 qubit | Single-Sided, Bottom | 0.583 | 12% |

### C. *Improvements due to Double-Sided Attack*

Table I also demonstrates the improvement of double-sided attack compared to single-sided attack. The table shows that double-sided crosstalk attack on average causes the total variational distance to increase 13% compared to only one sided attack. The maximum increase was 35%. Further, in some tests the increase was up to 223%, however, this may be an outlier and was not used in computing the average.

## V. Conclusion

This work presented a novel security attack based on $CNOT$ gate-induced crosstalk in superconducting qubit systems. Compared to previous studies, it introduced a double-sided crosstalk attack, where the attacker's circuits were placed on either side of the victim circuit executing in a multi-tenant, cloud-based quantum computer. A key innovation of this attack lay in the placement of the attacker's circuits on both sides of the victim. Experimental validation on cloud-based Rigetti quantum devices demonstrated that such attacks could compromise data integrity and cause changes in the outputs of the victim's circuit. The evaluation presented in this paper showed that the double-sided crosstalk attack on average causes the total variational distance to increase 13%, while the maximum increase was 35%, ignoring outliers which were even higher. These results underscored the dangers of crosstalk attacks, and the need for improved isolation mechanisms and secure scheduling policies in multi-tenant quantum cloud environments.

## References

[1] "Ibm quantum," https://quantum-computing.ibm.com/.

[2] "Amazon braket," https://aws.amazon.com/braket/.

[3] "Azure quantum," https://azure.microsoft.com/en-us/products/quantum.

[4] "Rigetti computing," https://www.rigetti.com.

[5] "Google quantum ai," https://quantumai.google.

[6] P. Das, S. S. Tannu, P. J. Nair, and M. Qureshi, "A case for multi-programming quantum computers," in *Proceedings of the 52nd Annual IEEE/ACM International Symposium on Microarchitecture*, 2019, pp. 291–303.

[7] S. Deshpande, C. Xu, T. Trochatos, H. Wang, F. Erata, S. Han, Y. Ding, and J. Szefer, "Design of quantum computer antivirus," in *Proceedings of the International Symposium on Hardware Oriented Security and Trust*, ser. HOST, May 2023.

[8] A. Ash-Saki, M. Alam, and S. Ghosh, "Analysis of crosstalk in nisq devices and security implications in multi-programming regime," in *Proceedings of the ACM/IEEE International Symposium on Low Power Electronics and Design*, 2020, pp. 25–30.

[9] "Hacking quantum computers with row hammer attack," 2025.

[10] "Context switching for secure multi-programming of near-term quantum computers," 2025.

[11] A. Li, S. Stein, S. Krishnamoorthy, and J. Ang, "Qasmbench: A low-level quantum benchmark suite for nisq evaluation and simulation," *ACM Transactions on Quantum Computing*, vol. 4, no. 2, pp. 1–26, 2023.