I Know What You Are Reading: Evaluating Readout Crosstalk in Cloud-based Quantum Computers

Yizhuo Tan
Yale University
New Haven, CT, USA
yizhuo.tan@yale.edu

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

Abstract

Frequency-multiplexing is a technique used for achieving resource-efficient readout in superconducting-based quantum computers. By enabling multiple resonators to share a common feed line, it significantly reduces the number of required cables and passive components. However, this gain in scalability introduces increased readout crosstalk. The readout crosstalk is not only a reliability issue, but also a possible security issue. Prior work has explored readout crosstalk in experimental systems not publicly available. This work builds on the prior findings and evaluates readout crosstalk in commercial, cloud-based quantum computers. In the process, this work also reconstructs the likely architecture for the shared readout feed lines and shows which qubit readout resonators likely share a feed line. This work finally shows that crosstalk-induced errors occurring during readout can be exploited by adversaries to infer the state of co-located victim qubits, leading to unintended information leakage.

CCS Concepts

• **Security and privacy → Side-channel analysis and countermeasures**.

Keywords

Quantum Computing, Readout Crosstalk

ACM Reference Format:
Yizhuo Tan and Jakub Szefer. 2025. I Know What You Are Reading: Evaluating Readout Crosstalk in Cloud-based Quantum Computers . In *Proceedings of the 2025 Quantum Security and Privacy Workshop (QSec '25), October 13–17, 2025, Taipei, Taiwan.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3733825.3765280

1 Introduction

Superconducting-based qubit quantum computers require highly controlled environments, such as cryogenic temperatures or ultra-high vacuum chambers, to maintain long qubit coherence times and enable high-fidelity control and readout. These systems also depend on intricate and costly control and measurement infrastructure, which often necessitates routine maintenance by trained specialists. Such operational complexities pose significant barriers to on-premises deployment of quantum hardware. To address these challenges, the cloud-based quantum computing paradigm has emerged, wherein quantum computers are hosted and accessed remotely. Major cloud providers such as IBM Quantum [9], Amazon Braket [2], Microsoft Azure Quantum [4], and Rigetti Computing [16] offer such remote access to various quantum computers, also called Quantum Processing Units (QPUs). In these environments, QPUs are shared resources, currently time-multiplexed among multiple users. Clients submit their quantum circuits for execution to the cloud provider, the circuits are run on a QPU, after which the QPU is reallocated to serve other users.

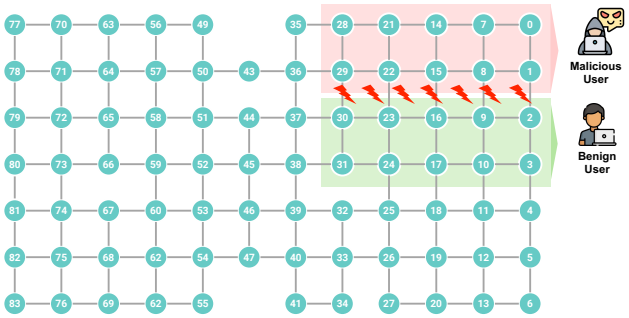


Figure 1: High-level diagram of a malicious attacker user co-located with a benign victim user malicious circuits on a quantum computer. The example attacker and victim locations are overlaid on top of the Rigetti Ankaa-3 quantum computer topology.

1.1 Motivation

The main model for cloud-based quantum computing services today is the time-sharing model wherein a single user is granted exclusive access to the quantum processor for a fixed duration of time. While straightforward, this model suffers from significant inefficiencies. The core limitation arises from the limited gate fidelities of current quantum hardware, which restrict multi-qubit entanglement to small subsets of qubits, often limiting usable quantum circuits to a few tens of qubits. As a result, a large fraction of available qubits remain idle during most executions.

Although not currently available from major quantum computer providers, multi-tenant QPUs have been actively explored in research [6] as one way to overcome the limitations of time-sharing model. In the multi-tenant setting, multiple users can execute their qubits on disjoint set of qubits, improving utilization of the quantum computer chips. 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

QSec '25, Taipei, Taiwan

ACM ISBN 979-8-4007-1913-4/2025/10
https://doi.org/10.1145/3733825.3765280

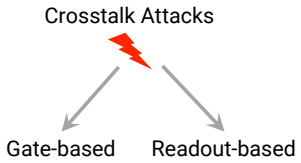


Figure 2: Main crosstalk attack types.

this work is to help better understand the potential security threats in multi-tenant quantum computers, focusing on readout crosstalk.

1.2 Security Issues Cloud-based Quantum Computers

Figure 1 shows a high-level picture of the threats in shared quantum computers. As demonstrated in the figure, when two users execute their circuits on a quantum computer, unintended (or malicious) noise between the two circuits can negatively impact the execution of a user's circuit. This noise can be generally called crosstalk.

Figure 2 further shows that there are two types of crosstalk in quantum computers. Gate-based crosstalk occurs when quantum gate are execute on certain qubits, and that affects other qubits. Readout-based crosstalk occurs when qubit readout circuits share feed lines, and this allows some qubits to affect readout values of other cubits sharing the feed line.

Most of the academic work so far has focused on gate-based crosstalk and attacks. Prior gate-based crosstalk attacks which have considered typically one attacker circuit located on one side of the victim [3, 7], or more recent [1] work focused on using two attacker circuits. In almost all cases, the attacker is a circuit that uses a lot of *CNOT* gates to generate noise that affects near-by qubits. Only recently is more attention paid to the readout crosstalk that was explored in [14].

According to existing work [14], readout-based crosstalk arises from a combination of physical and electronic interactions. Key contributing factors include: (a) interference between concurrent readout probe signals, (b) residual photon population induced by coupling to neighboring probe tones or readout resonators, (c) unintended coupling between a readout resonator and adjacent qubits, and (d) signal interactions occurring in the readout chain, such as in amplifiers, mixers, or during analog demodulation and digitization. Collectively, these effects degrade measurement fidelity and introduce correlated errors across qubits. When the qubits belong to different users, these correlated errors become a form of side-channel for information leakage.

1.3 Results Highlight and Contributions

To best of our knowledge, this is the first work that attempts to analyze readout crosstalk in commercial, cloud-based quantum computers. In particular, we use qBraid to access the Rigetti Ankaa-3 quantum computer via the Amazon Braket cloud service. In addition, and in order to analyze the readout crosstalk, we perform tomography experiments on Rigetti Ankaa-3 to estimate which qubit readout circuits may be sharing feed lines. Thus we believe this to be the first work that aims to show that it could be possible to estimate the hardware configuration of quantum computer through remote experimentation. In the end, we demonstrate an end-to-end example where multiple bits are leaked through the readout crosstalk side-channel.

2 Threat Model

We consider a cloud-based, multi-tenant quantum computing platform that allows multiple users to submit and execute quantum programs concurrently on a shared physical quantum computer. Each user is logically isolated and interacts with the system through standard interfaces, with no direct access to the underlying hardware or to other users' code or data. The adversary in our model is a malicious tenant who submits specially crafted quantum programs with the goal of extracting information about co-resident users' computations or it's outputs. The adversary is assumed to have no privileged access to the control stack or backend, but can exploit physical-layer effects, such as readout crosstalk, shared control lines, or measurement-induced correlated errors, to infer or influence victim qubits. This model is analogous to side-channel threats in classical cloud systems, where physical resource sharing introduces unintended communication channels between isolated workloads. We do not assume denial-of-service as the primary objective, though such attacks may emerge as a byproduct.

3 Evaluation Setup

In this work we evaluate readout crosstalk on Rigetti Ankaa-3 quantum computer available for cloud-based access from Amazon Braket. All the evaluation is performed remotely by running Python notebooks on the qBraid platform.

3.1 Quantum Computer Hardware Used

We use Ankaa-3, which is Rigetti Computing's latest superconducting quantum processor, featuring 84 qubits arranged in a square lattice topology with tunable couplers. Designed for high-performance multi-qubit operations, Ankaa-3 achieves a median two-qubit iSWAP gate fidelity of approximately 99.0% and a median fSim gate fidelity of 99.5% [17]. Gate durations are notably fast, with iSWAP and fSim gates operating at median durations of 72ns and 56ns, respectively. These performance gains are enabled by a redesigned hardware stack, including enhanced cryogenic packaging, improved thermalization and shielding, and precise Josephson junction fabrication using Alternating-Bias Assisted Annealing (ABAA). Ankaa-3 also incorporates a precision control stack capable of real-time pulse pre-compensation and dynamic frequency optimization for both qubits and couplers.

Ankaa-3 is currently accessible via Rigetti Quantum Cloud Services (QCS), as well as through Amazon Braket. All Amazon Braket quantum computers from various vendors are further usable from qBraid, which is a cloud-based quantum computing platform that provides users with unified access to quantum hardware and software development tools.

3.2 Quantum Computer Testing Circuits

We leverage simple test circuits to evaluate possible readout crosstalk. The test circuits only use X gates when we want to initialize a qubit to $|1\rangle$ or no gates when the qubit is left if $|0\rangle$. They further use measurements to trigger qubit readout. No special gates nor control

sequences are used. The test circuits are described in detail in the following sections along with the location of the qubits tested.

4 Mapping Shared Readout Feed Lines

Before evaluating the readout crosstalk, we need to first analyze the target quantum computer to gain understanding of which may be the shared feed lines. We were unable to find documentation for Rigetti Ankaa-3 that shows which are the shared feed lines. As result, we developed a set of experiments to analyze which qubits may be sharing feed lines.

4.1 Shared Readout Feed Lines

A schematic of a shared readout line is shown in Figure 4. Multiple qubits are connected to their readout resonators which then share a purcell filter. According to existing work [14] qubits which share the readout lines experience noise and interference. Shared readout feed lines can in particular manifest themselves when there is state-dependence of crosstalk between target and spectator qubits both of which share the readout line.

4.2 Detecting Shared Readout Lines

To find possible shared feed lines, we need to find pairs or sets of qubits where the readout value of a spectator qubit seems to be heavily affected by the state of the target qubit [14]. If qubits share a feed line, then a $|1\rangle$ value on the target qubit will affect the readout out value of the spectator qubit, while $|0\rangle$ will have limited effect on the spectator qubit. As a result, we want to test various sets of qubits where we fix the spectator qubit to $|0\rangle$ and then set target qubits to either $|1\rangle$ or $|0\rangle$ and observe any combinations where the spectator qubit has higher chance of being read in state $|1\rangle$.

4.3 Testing Strategy

Due to cost constraints, it is not feasible to exhaustively test all the possible combinations of qubits one by one. In particular, one job of 1000 shots costs about 1.2 USD on Rigetti Ankaa-3 machine, thus the testing costs quickly increase as we run many jobs. To address this issue, we test multiple qubits at a time.

In our testing strategy, one qubit set in $|0\rangle$ state is used as the spectator, and multiple qubits are used as target qubits. Among the target qubits, we perform multiple experiments where different subsets of target qubits are set to either $|0\rangle$ or $|1\rangle$. For each experiment we run it for 1000 shots and collect output probabilities for the spectator qubit. From the output probabilities we observe how many times the spectator qubit was read out in $|1\rangle$ state. Higher number indicates that there may be readout crosstalk among the target qubits and the spectator qubit. However, in each experiment, different sets of target qubits are used. Thus we need to find which of these target qubits have the highest impact on the spectator. We treat this problem of finding which target qubits have highest impact on the spectator qubit as a feature attribution problem.

The feature attribution problem is set up as follows. For a given spectator qubit, we have a fixed pattern of target qubits, shown in Figure 3. For each test, we set all the target qubits used in that test to $|0\rangle$ and collect the measurements and then set all the target qubits used in that test to $|1\rangle$ and again collect measurements. For each test i we compute Δ_i as the increase in spectator qubits measured as $|1\rangle$. For example, for a test i, if spectator is measured in $|1\rangle$ state 40 out of 1000 shots when target qubits are in $|0\rangle$ and it is measured in $|1\rangle$ state 310 times when the target qubits are $|1\rangle$ then the Δ_i is 270.

Table 1: Highly correlated qubits associated with each spectator qubit. Please reference Figure 2 for the qubit numbers and their location within the Ankaa-3 topology.

Spectator Spectator	Highly Corr. Qubit 1	Highly Corr. Qubit 2	Highly Corr. Qubit 3
8	15	9	1
9	10	16	2
15	8	14	22
16	23	15	9

With the collected data and the Δ_i values for all the different tests, we use a Random Forest Regressor, a supervised machine learning algorithm, to find which target qubits have the highest impact on the spectator qubit. This is in effect determining the feature importance. Each target qubit is treated as a feature, and the Δ_i values are the scores. The machine learning algorithm is used to evaluate which features (i.e. target qubits) best correlate with the scores.

4.4 Likely Shared Readout Lines

Due to the extensive value of running jobs on the Ankaa-3 quantum computer, we have tested four spectator qubits within the quantum computer, qubits: 8, 9, 15, and 16. For each spectator qubit we employed the strategy shown in Figure 3. As result, for each spectator qubit, we have data for 8 target qubits which are located adjacent to it in the square lattice topology. We used the Random Forest Regressor to find for each spectator qubit, the top 3 target qubits that seem to have the highest impact or influence on causing the spectator qubit's output to change from $|0\rangle$ to $|1\rangle$. The correlation between the target and spectator qubits is shown in Table 1.

Based on the data from the table, we find a repeating pattern that is shown in Figure 5. Readout of qubits 8 and 9 in the second column from the right in the topology of Ankaa-3 is strongly related to the state of the qubits on the left, right and bottom of the spectator qubit. In the third column from the fight in the topology of Ankaa-3, readout of the qubits 15 and 16 is strongly related to the state of the target qubits above, to the right and left of the spectator qubit. The overlap of the high correlated qubits indicates that possible qubits 8 and 15 share a readout line and qubits 9 and 16 share a readout line. We do not have access to proprietary data from Rigetti to validate these claims, however, experimentally there is this relationship that we observe.

5 Readout Crosstalk Side Channel Results

Having found interesting correlation between the target and spectator qubits, we now evaluate a simple readout crosstalk side channel.

5.1 Victim Circuit

The victim circuit we use is a 2-qubit Grover's circuit. Grover's algorithm is a quantum algorithm designed to provide speedup

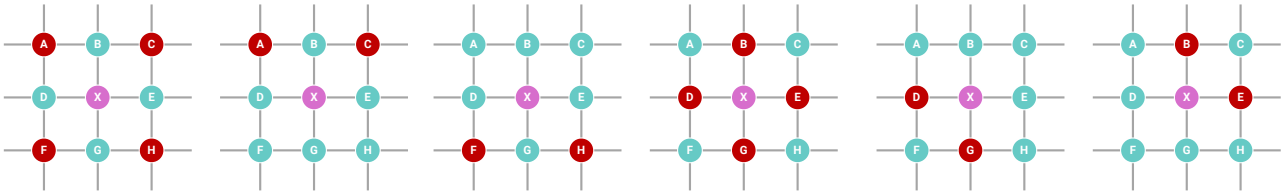


Figure 3: Mapping shared readout feed lines testing strategy: x is the spectator qubit, while the red qubits are different target qubits used in each test. For each tests, two sets of measurements are taken, with all target qubits in $|0\rangle$ state, and with all target qubits in $|1\rangle$ state. In total there are 12 sets of data for each spectator qubit: 6 tests $\times$ 2 two sets of measurements.

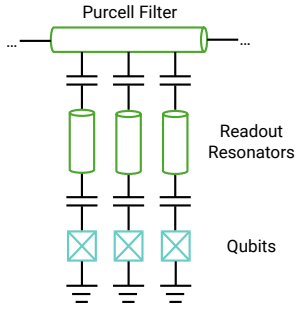


Figure 4: Schematic of a shared readout feed line, figure made after [5].

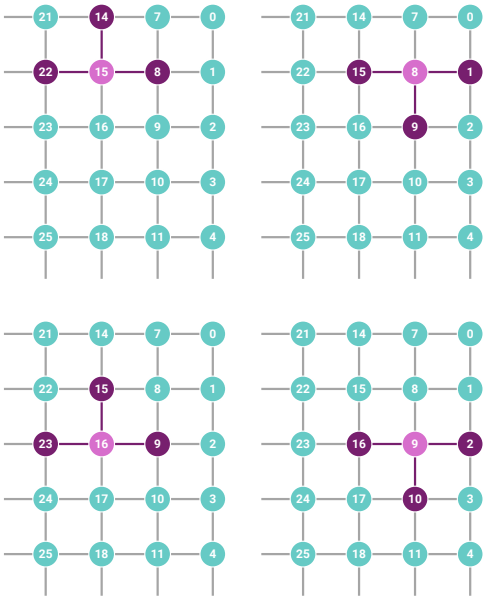
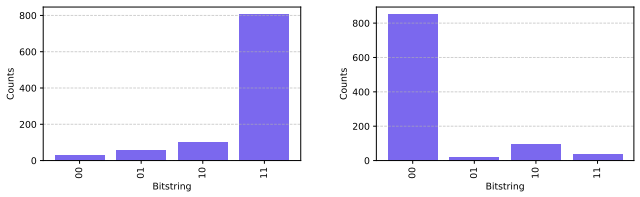


Figure 5: Readout crosstalk.

when searching in an unsorted database. For 2 qubits, the database has $n = 4$ items and an oracle within the Grover's algorithm can be used to mark one of the items: 00, 01, 10, or 11. We execute the 2-qubit Grover's circuit on qubits 15 and 16 of Ankaa-3.



(a) Grover's output probabilities for target state 11.

(b) Grover's output probabilities for target state 00.

Figure 6: Output probabilities for victim Grover's algorithm on qubits 15 and 16.

5.2 Attacker Circuit

The attacker circuit is a 2-qubit circuit which has no gates and it is a simple circuit that simply performs measurement of its qubits. Since the qubits are always initialized to $|0\rangle$ the output of the circuit should always be 00 with highest probability, unless there is crosstalk or other noise.

5.3 Attacker Circuit Locations

The attacker circuit is always executed in parallel to the victim circuit, each being executed for 1000 shots. We performed two tests: "near" attacker is placed on qubits 8 and 9. From the prior evaluation in Section 4.4 the qubits 15 and 8 likely share a readout line and qubits 16 and 9 likely share a readout line. Thus, when victim is on qubits 15 and 16 and attacker is on qubits 8 and 9, we expect the attacker's measurement to be affected by the victim's qubits' final state through the readout crosstalk.

In separate test, a "far" attacker was placed on qubits 71 and 72. As these qubits are far away from the victim qubits, and likely do not share readout lines, we expect the attacker's measurement to be not affected by the victim's state.

5.4 Stealing Grover's Results

We ran two sets of experiments. In one set, the target state for Grover's was set to 11 and in the other the target state was set to 00. The results can be seen in the Figure 6. The results correctly show that the dominant state is 11 and 00 respectively.

In parallel, we measured the attacker circuit. The attacker circuit has four possible output states, with 00 being most likely, unless there is crosstalk. We use variational distance to compare the output of the attacker when the victim's target state was set to 11 to when the target state was set to 00. Table 2 shows the results.

Table 2: Variational distance of attackers measurements, higher means there is more difference between when the victim is 11 and 00.

Attacker Type	Variational Distance
Near Attacker	0.026
Far Attacker	0.003

It can be observed that when we use a "far" attacker, the variational distance is 0.003 indicating that the outputs are almost the same regardless the state of the victim. Meanwhile, for the "near" attacker, the variational distance is 0.026, indicating that the output of the attacker is affected by the state of the victim. When the victim's output is 11 the attackers counts for 00 decrease from 944 to 918 (out of 1000 shots). The change is small, but could be used to detect and differentiate whether victim's Grover's output is 11 or 00, thus attacker may be able to steal Grover's circuit's results and violate confidentiality of the victim.

6 Related Work

The security of quantum computing, particularly in shared cloud environments, has rapidly evolved from a theoretical concern to an active and broad field of research. Our work on readout crosstalk side-channels contributes to a growing body of literature focused on understanding and mitigating vulnerabilities in the quantum computing stack. Our work builds upon several key areas of prior research: multi-tenant quantum computing, crosstalk attacks and other side-channel attacks.

Multi-Tenant and Cloud Quantum Computing Security: The foundation for our threat model is the multi-tenant execution paradigm, proposed to enhance the utilization of large QPUs [6]. This shared environment, however, introduces security risks. Recent work has focused on managing this shared space securely. Kumar et al. explore secure context switching [10], while Upadhyay et al. proposes a framework for secure hardware allocation and resource management [20]. Other efforts focus on optimizing job execution in this new paradigm, such as job splitting for higher fidelity and throughput [12]. These works highlight the operational drive towards multi-tenancy and the corresponding need for the security evaluations that our paper provides.

Crosstalk-Based Attacks: To date, most research into physical crosstalk as a security vector has focused on gate-based interference. Ash-Saki et al. first analyzed the security implications of gate crosstalk in a multi-programming regime [3]. This concept has since been evolved into more aggressive attacks. Almaguer-Angeles et al. [1] and Tan et al. [19] proposed "Quantum Rowhammer" and "QubitHammer" attacks, respectively, which use repetitive gate operations on attacker qubits to induce bit flips in victim qubits, drawing a direct parallel to classical DRAM attacks. Other works have explored adversarial SWAP gate injection as a physical attack vector [11, 21]. Our work deviates from this focus on gate-induced errors. We build directly upon the foundational analysis by Maurya et al. [14], who first identified readout architectures as a potential side-channel vulnerability on experimental systems. Our primary contribution is to provide the first experimental validation and end-to-end attack demonstration of readout crosstalk on a publicly accessible, commercial quantum computer, thereby proving its practical threat.

Other Side-Channel and Physical Layer Attacks: Beyond crosstalk, researchers have explored other physical side-channels. Xu et al. demonstrated that power side-channels from the classical control hardware can be used to reconstruct quantum circuits [8, 22]. Lu et al. showed the existence of timing side-channels in cloud-based quantum services [13]. Others have investigated vulnerabilities in the reset operation [15, 18] and the potential for "jailbreaking" attacks that exploit low-level control [23]. These studies complement our work by showing that the entire physical stack, from control electronics to the QPU itself, is a rich surface for side-channel attacks on quantum computer systems.

7 Conclusion

This work provides the first experimental evaluation of readout crosstalk as a security vulnerability on a cloud-based quantum computer. We demonstrated that the resource-sharing optimizations in modern superconducting QPUs, specifically the use of shared readout feed lines, can be exploited for information leakage. By systematically running experiments on the Rigetti Ankaa-3 processor, we developed a methodology to reverse-engineer the likely physical layout of these shared feed lines, identifying groups of qubits whose measurements are highly correlated.

Building on this reconstructed hardware mapping, we successfully demonstrated an end-to-end side-channel attack. By co-locating a simple measurement-only attacker circuit near a victim running a 2-qubit Grover's algorithm, the attacker was able to statistically distinguish between the victim's final output states. This information leakage, though small, confirms that readout crosstalk is not merely a theoretical risk or a reliability issue, but a tangible security threat on today's quantum hardware. As the quantum computing field progresses towards multi-tenant architectures to increase QPU utilization, our findings underscore the critical need for hardware and system-level mitigations to protect user computations from such side-channel attacks and ensure the confidentiality of cloud-based quantum computing.

Acknowledgments

This work was supported in part by NSF grant 2332406.

References

[1] Fernando Almaguer-Angeles, Pedro R. Dieguez, Akshata Shenoy H., and Marcin Pawłowski. 2025. Hacking quantum computers with row hammer attack. arXiv:2503.21650

[2] Amazon Braket [n. d.]. Amazon Braket. https://aws.amazon.com/braket/

[3] Abdullah Ash-Saki, Mahabubul Alam, and Swaroop Ghosh. 2020. 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*. 25–30.

[4] Azure Quantum [n. d.]. Azure Quantum. https://azure.microsoft.com/en-us/products/quantum.

[5] Liangyu Chen, Hang-Xi Li, Yong Lu, Christopher W Warren, Christian J Križan, Sandoko Kosen, Marcus Rommel, Shahnawaz Ahmed, Amr Osman, Janka Biznárová, et al. 2023. Transmon qubit readout fidelity at the threshold for quantum error correction without a quantum-limited amplifier. *npj Quantum Information* 9, 1 (2023), 26.

[6] Poulami Das, Swamit S Tannu, Prashant J Nair, and Moinuddin Qureshi. 2019. A case for multi-programming quantum computers. In *Proceedings of the 52nd Annual IEEE/ACM International Symposium on Microarchitecture*. 291–303.

[7] Sanjay Deshpande, Chuanqi Xu, Theodoros Trochatos, Hanrui Wang, Ferhat Erata, Song Han, Yongshan Ding, and Jakub Szefer. 2023. Design of Quantum Computer Antivirus. In *Proceedings of the International Symposium on Hardware Oriented Security and Trust (HOST)*.

[8] Ferhat Erata, Chuanqi Xu, Ruzica Piskac, and Jakub Szefer. 2024. Quantum Circuit Reconstruction from Power Side-Channel Attacks on Quantum Computer Controllers. In *Transactions on Cryptographic Hardware and Embedded Systems (TCHES)*.

[9] IBM Quantum [n. d.]. IBM Quantum. https://quantum-computing.ibm.com/.

[10] Avinash Kumar, Meng Wang, Chenxu Liu, Ang Li, Prashant J. Nair, and Poulami Das. 2025. Context Switching for Secure Multi-programming of Near-Term Quantum Computers. arXiv:2504.07048

[11] Wei Jie Bryan Lee, Siyi Wang, Suman Dutta, Walid El Maouaki, and Anupam Chattopadhyay. 2025. SWAP Attack: Stealthy Side-Channel Attack on Multi-Tenant Quantum Cloud System. arXiv:2502.10115

[12] Jinyang Li, Yuhong Song, Yipei Liu, Jianli Pan, Lei Yang, Travis Humble, and Weiwen Jiang. 2025. QuSplit: Achieving Both High Fidelity and Throughput via Job Splitting on Noisy Quantum Computers. arXiv:2501.12492

[13] Chao Lu, Esha Telang, Aydin Aysu, and Kanad Basu. 2025. Quantum leak: Timing side-channel attacks on cloud-based quantum services. In *Proceedings of the Great Lakes Symposium on VLSI 2025*. 252–257.

[14] Satvik Maurya, Chaithanya Naik Mude, Benjamin Lienhard, and Swamit Tannu. 2024. Understanding Side-Channel Vulnerabilities in Superconducting Qubit Readout Architectures. In *2024 IEEE International Conference on Quantum Computing and Engineering (QCE)*. IEEE, 1177–1183. doi:10.1109/qce60285.2024.00138

[15] Allen Mi, Shuwen Deng, and Jakub Szefer. 2022. Securing Reset Operations in NISQ Quantum Computers. In *Proceedings of the Conference on Computer and Communications Security (CCS)*.

[16] Rigetti Computing [n. d.]. Rigetti Computing. https://www.rigetti.com.

[17] Rigetti Computing. 2024. Rigetti Computing Launches 84-Qubit Ankaa-3 System, Achieves Record Performance. https://investors.rigetti.com/news-releases/news-release-details/rigetti-computing-launches-84-qubit-ankaatm-3-system-achieves Accessed: 2025-07-09.

[18] Jerry Tan, Chuanqi Xu, Theodoros Trochatos, and Jakub Szefer. 2024. Extending and defending attacks on reset operations in quantum computers. In *2024 International Symposium on Secure and Private Execution Environment Design (SEED)*. IEEE, 73–83.

[19] Yizhuo Tan, Navnil Choudhury, Kanad Basu, and Jakub Szefer. 2025. QubitHammer Attacks: Qubit Flipping Attacks in Multi-tenant Superconducting Quantum Computers. arXiv:2504.07875

[20] Suryansh Upadhyay and Swaroop Ghosh. 2024. Share: Secure hardware allocation and resource efficiency in quantum systems. In *2024 IEEE International Conference on Quantum Computing and Engineering (QCE)*, Vol. 1. IEEE, 1109–1119.

[21] Suryansh Upadhyay and Swaroop Ghosh. 2024. Stealthy SWAPs: Adversarial SWAP Injection in Multi-Tenant Quantum Computing. In *International Conference on VLSI Design and International Conference on Embedded Systems (VLSID)*. 474–479.

[22] Chuanqi Xu, Ferhat Erata, and Jakub Szefer. 2023. Exploration of Power Side-Channel Vulnerabilities in Quantum Computer Controllers. In *Proceedings of the Conference on Computer and Communications Security (CCS)*.

[23] Chuanqi Xu and Jakub Szefer. 2024. Jailbreaking Quantum Computers. (2024). arXiv:2406.05941