Hacking quantum computers with row hammer attack

Fernando Almaguer-Angeles ⓘ,[1, *] Pedro R. Dieguez ⓘ,[1, †] Akshata Shenoy H. ⓘ,[1, ‡] and Marcin Pawłowski ⓘ[1, §]

[1]*International Centre for Theory of Quantum Technologies,*
University of Gdańsk, Jana Bażyńskiego 1A, 80-309 Gdańsk, Poland
(Dated: March 28, 2025)

We demonstrate a hardware vulnerability in quantum computing systems by exploiting cross-talk effects on an available commercial quantum computer (IBM). Specifically, based on the cross-talk produced by certain quantum gates, we implement a row hammer attack that ultimately allows us to flip a qubit. Both single-qubit and two-qubit operations are performed and analyzed. Our findings reveal that two-qubit operations applied near the target qubit significantly influence it through cross-talk, effectively compromising its state.

Quantum computing is advancing towards real-world applications [1, 2], promising unprecedented processing power [3] with potential breakthroughs in fields such as cryptography [4], material science [5, 6], and artificial intelligence [7]. However, as these systems become more integrated into infrastructures involving sensitive data processing, security concerns grow [8–10]. Modern computing systems rely on confidentiality, integrity, availability, and safety of critical processes [11–13], making it essential to assess and mitigate potential vulnerabilities. In fact, quantum computers (QC) are vulnerable to integrity attacks [14–16]. QCs are susceptible to *cross-talk*, a phenomenon in which unintended interactions between the nearest neighboring qubits can compromise their computational accuracy and reliability. Understanding and mitigating these vulnerabilities is essential in determining whether quantum computing can be trusted for critical applications.

In quantum computing, cross-talk occurs when one component of an experimental setup—such as a qubit, control line, electromagnetic field, resonator, or photodetector—unintentionally influences another [17]. These unintended interactions can introduce errors, compromise computational accuracy, and, more critically, be exploited as a security vulnerability. Here, we explore the quantum counterpart of the well-known *row hammer attack*, a hardware vulnerability commonly exploited in classical computing. In classical systems, a row hammer attack involves repeatedly accessing specific memory rows to induce bit flips in adjacent memory locations. These unwanted bit-flip errors in neighboring rows, known as target rows, increase with the number of devices per area on a hardware unit. Row hammer attacks have been attempted with repetitive access to single, two, or multiple targets [18]. It is known that refreshing the target rows repetitively provides a simple yet inefficient solution to the issue. There exists other complex software-based countermeasures as well though all of them do not entirely solve the problem [19].

Row hammer attacks have been used to escalate privileges and execute system calls beyond a sandbox, allowing access to a limited subset of x86-64 machine instruc-
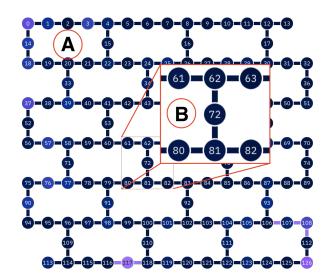

FIG. 1. A: IBM's QC qubit topology. B: Example of the structure to be used in the experiments. Grid of qubits, represented by numbered circles, and their physical connection, represented by a line connecting two qubits in a topological arrangement of 127 qubits.

tions [20]. A report from the CVE Program [21], a cybersecurity vulnerability database, described an incident in October 2016 where an Android application exploited row hammer, among other techniques, to gain root access on several popular smartphones. The vulnerability stems from the physical limitations of the newer DRAM chips. In response, Google's security research team disclosed a new row hammer exploit [22], highlighting the ongoing risks associated with this attack. Security researchers have further demonstrated that row hammer exploits can be independent of both system architecture and instruction set [23].

In this letter, we demonstrate how to exploit cross-talk in IBM's QC architecture shown in Fig. 1 by designing a row-hammer attack to compromise it. Specifically, we investigate whether it is possible to flip a target qubit by applying a set of universal quantum gates (**QG**). To explore this vulnerability, we implement both single-qubit rotations and two-qubit operations. Fo-

cusing on controlled-not (**C-Not**) gates, our results reveal that significant cross-talk can be induced allowing flipping of a qubit with high probability. To validate our approach, we conduct experiments on three different IBM QC, analyze their chip architecture, and design row hammer attacks. We provide a detailed algorithm for the attack ensuring reproducibility of quantum circuits. A Cramér's V statistical analysis is also performed to assess its feasibility in establishing a cause and effect of using these gates to induce crosstalk. The results are divided into two main parts. The first verifies whether or not single qubit gates induce sufficient cross-talk. The second part explores cross-talk produced by a two-qubit gate such as the C-Not. Our findings demonstrate the potential security risks posed by cross-talk in QCs and highlight the need for improved mitigation strategies.

Experiments- The experiments were run in *Brisbane*, *Kyiv*, and *Sherbrooke* IBM's QCs, with a 10-minutes free-usage monthly account, and Qiskit *sampler* method. All IBM's QCs used in this work have the same qubit topology, and can be seen in Fig. 1 A. Certain Points were chosen to increase cross-talk and perform the experiments. These points followed Fig. 1 B, where QG were put around the *centre*. Giving us a total of 18 centres. For simplicity, we choose uniformly only six centres to collect data from to demonstrate the vulnerability. These are 15, 34, 54, 72, 93, and 109.
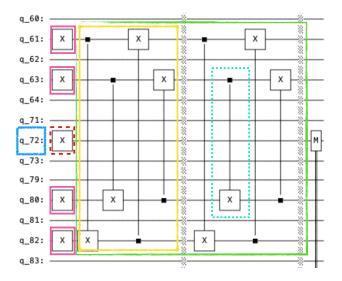

FIG. 2. The Experiment: In the above circuit, the pink box indicates state preparation. The cyan box marks the gate operations that are involved. While the red dashed box shows the initial state of the measuring qubit, the blue box represents the target qubit to be flipped and the green box encompasses the number of additional gate sets applied. Finally, the Yellow box defines the base experiment setup, specifying the gate type and arrangement.

The experimental circuit is labeled as follows. In Fig. 2, the pink boxes indicate that the qubits have been initialized in the state $|1\rangle$ as opposed to the default $|0\rangle$

in IBM QC. The blue box indicates the target qubit q_{72} which has been initialized in $|1\rangle$ as indicated by the red dashed box. The green box represents the full-structure gate that will be employed in the present case. The yellow box represents the primary gates that were used. The configuration depicted in Fig. 2, the target qubit is labeled -cx(-72-1) 4 *cross*[1] because the involved operation qubits form a cross in the chosen subtopology of qubits 61, 63, 80, and 82.

The experiments are aimed to measure cross-talk on IBM QCs by performing various gate operations around a central qubit and measuring its output. An example of this setup is illustrated in Fig. 3, where the central qubit is chosen to be 72 which is surrounded by other qubits (according to the topology 61, 62, 63, 80, 81, and 82), which were involved in the gate operations. Two types of gates were used in these experiments: single-qubit gates and the two-qubit C-Not gate.
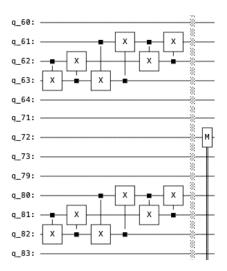

FIG. 3. An example of a quantum circuit using a suitable subtopology in IBM's QC. The set-up demonstrates how a C-Not gate's cross-talk can be employed to orchestrate a row hammer attack and flip a qubit.

For the single-qubit gate experiments, P, RZ, RX, RY, $\sqrt{x}$, $\sqrt{x}^{\dagger}$, Y, and U gates were chosen. The definition of these gates can be found in the Appendix A. The experiments were conducted using different configurations, each with an increasing number of gates. Every experiment was repeated $40,000$ times, measuring only the output of the target (central) qubit. Due to the complexity of the configurations and the large number of executions, specialized factory-style software was used to generate quantum circuits consistently in a reproducible manner. The algorithm behind this software is presented in Appendix B.

————

[1][pink]-[cyan]cx([red]-[blue]72-[green]1) [yellow]4 *cross*

Errors in IBM's QCs can be classified into two main categories. The first category involves hardware errors which include metrics such as error per layered gate, readout assignment error, probability of measuring 0 when preparing $|1\rangle$, Z-axis rotation (rz) error, $\sqrt{x}$ (sx) error, Pauli-X error, and ECR error, among others [24]. The second category pertains to software-induced errors, particularly those associated with Python-based Qiskit. IBM continuously monitors and recalibrates hardware metrics through its calibration data processes. To account for these fluctuations, a control experiment was included in each experimental round to assess the QC's precision at that specific moment. This control data provides a baseline for output comparison, helping to identify the presence of cross-talk. In contrast, the errors related to IBM's sampler method are non-physical, meaning they are not used to evaluate readout or gate performance. Instead, these errors manage the program's logic flow and provide feedback to software developers. For instance, they include errors such as *invalid arguments given*, which are not tied to the hardware's physical behavior but ensure the proper execution of the quantum program [24].

Results- The results of the experiments are presented as follows. First, the data from the single-qubit experiments are used for the rest of the analysis. Second, the most representative two-qubit setup experiment is explained, while experimental results using the other two QCs are presented in Appendix D.

The collected data is stored in a CSV file similar to Table I. This table illustrates the gate sets around the

Experiment	Output 0 %	Output 1 %
Precision(93)	97.2675	2.7325
p(93-1000) 6	97.365	2.635
rz(93-1000) 6	97.365	2.635
rx(93-1000) 6	96.7325	3.2675
ry(93-1000) 6	96.6425	3.3575
$\sqrt{x}$(93-1000) 6	96.9575	3.0425
$\sqrt{x}^{\dagger}$(93-1000) 6	96.995	3.005
y(93-1000) 6	96.245	3.755
u(93-1000) 6	96.6875	3.3125

TABLE I. Brisbane single-qubit experiments results.

central qubit (in this example, $1,000$ additional sets are included), denoted as qubit 93 in the *Experiment* column. The *Output* columns represent the observables measured in these experiments. Since the experiments focused on a qubit not undergoing any operations, an Output 0 was expected. Increasing inaccuracy in expectation values between distant qubits reveals the level of noise present, as discussed in previous studies [25, 26]. Therefore, as higher the percentage of Output 1, the higher of qubit flipping and success of the row hammer attack.

Table I demonstrates that the experiment is stable and does not induce cross-talk to adjacent channels. This stability is also observed in the results from the Kyiv quantum processors, details in Appendix C. However, Sherbrooke is an exception, giving us more than 82.89% of qubit flipping. Yet, these results are achieved at the cost of lower precision, which in this experiment is 83.35%. This indicates that the single-qubit method would not be effective for conducting a successful row hammer attack due to the number of single-qubit gates required.
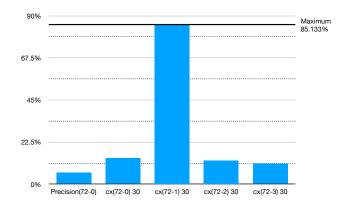

FIG. 4. Sherbrooke A: Flipping $|0\rangle$ to $|1\rangle$. Successful rate of 40,000 experiments on qubit flipping using different C-Not gates setups on a specific IBM QC.

Sherbrooke's analysis, for the C-Not gate, includes two different objectives. On the one hand, in Figs. 4 - 5, the target qubits are being tried to be flipped from $|0\rangle$ to $|1\rangle$. Fig. 4, depicts one such successful attack. It was performed on centre 72 with 30 C-Not configuration and one extra set, obtaining a bit flip for more than 85.13%. In Fig. 5, we have four successful attacks. Configuration using 30 C-Not gates around qubit 72, two Hadamard gates on qubits 61, and 63, on the top qubit row, and in the same fashion on the bottom qubit row, and no extra sets, has a little less than 76.39% of successful qubit flip. Another successful configuration is a four-gate cross configuration, an extra set of gates, around qubit 72 that has slightly more than 87.35% of qubit flip. The last successful configuration has two configurations, which is a 30 C-Not gate configuration with two and three extra gate sets, one Hadamard gate at qubit 62 on the top, and one at the bottom on qubit 81. The first of these configurations has less than 84.35% of qubit flip, while the second has more than 86.65% of qubit flip.

The results indicate that both configurations, with and without entanglement, led to successful attacks, making it unclear whether the entanglement produced by C-Not gates play a significant role in the attack. On the other hand, in Fig. 6, attempts to the flip qubit from $|1\rangle$ to $|0\rangle$, shows only one successful event for the $cx(-72-0)30$ configuration. It has a slightly more than 90.81% of observing qubit flip. It is worth mentioning that these ex-

periments have a precision of 93.83% for Fig. 4, while for the rest of the plots, above 83.31%. Therefore, these flipping qubit percentages occurred with a relatively high precision. Moreover, to determine whether these categorical variables are correlated, a Cramér's V analysis is detailed in Appendix E.
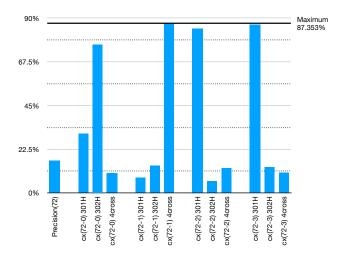

FIG. 5. Sherbrooke B: Flipping the state $|0\rangle$ to the $|1\rangle$. Successful rate of 40,000 experiments on qubit flipping using different C-Not gates setups on a specific IBM QC.
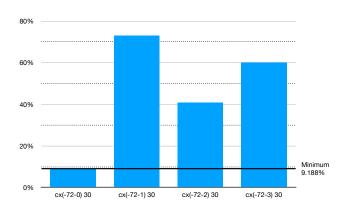

FIG. 6. Sherbrooke: Flipping the state $|1\rangle$ to the $|0\rangle$. Successful rate of 40,000 experiments on qubit flipping using different C-Not gates setups on a specific IBM QC.

The previous results led to further experiments, which were conducted at the previously selected centers using the successful attack settings. Figs. 7 - 8 show these centres and the flipping percentage on the different settings. Fig. 7 shows only one successful attack. Configuration $cx(15 - 1)4$ cross has a qubit flipping rate of a bit more than 89.09%, and a precision of 92.44%. Fig. 8 shows three successful attacks. The first one, with slightly more than 87.40% configuration cx(-15-0)30, has a precision of 92.44%. The second one is $cx(-34 - 0)30$ with 78.42% of qubit flipping and a precision of more than 83.21%. The last one is $cx(-54 - 0)30$ with a successful qubit flipping
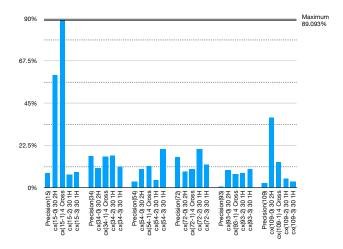

FIG. 7. Sherbrooke: Flipping the state $|0\rangle$ to the $|1\rangle$ on different centres. Successful rate of 40,000 experiments on qubit flipping using different C-Not gates setups on a specific IBM QC.

rate of more than 75.31%, and a precision of a little over 96.73%. The results for Kyiv and Brisbane QC are shown on Appendix D.
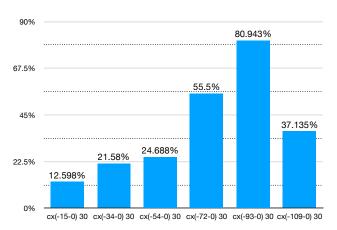

FIG. 8. Sherbrooke: Flipping $|1\rangle$ to $|0\rangle$ on different centres. Successful rate of 40,000 experiments on qubit flipping using different C-Not gates setups on a specific IBM QC.

These experiments have been classified as row hammer attacks due to the repeated application of quantum operations to induce unintended state changes in the target qubit. Specifically, we executed 40,000 operations on the target qubit, analogous to the repeated memory accesses in classical row hammer attacks. This persistent "hammering" exploited cross-talk effects to manipulate the target state. In the most effective cases, this method achieved a success rate of just under 94.83%, demonstrating the reliability of the attack in inducing controlled bit flips.

Discussion- In this letter, we showed how to perform a successful row hammer attack on a QC by using certain QG and cross-talk to flip a qubit. This represents a

significant security risk, as QCs are expected to handle sensitive applications, including cryptographic tasks and blind computation. The ability to flip a qubit undermines the reliability of quantum operations and raises concerns about the trustworthiness of quantum computations.

To address this issue, further research is needed to fully understand the mechanisms behind cross-talk-induced attacks, develop reliable detection methods, and implement effective countermeasures. Future studies should explore mitigation strategies, such as optimized qubit layouts, error-correcting protocols, and hardware-level solutions to minimize cross-talk effects. As quantum technology advances, ensuring its security and resilience against such vulnerabilities will be crucial for its safe and reliable adoption in critical applications.

Appendix A: Single-qubit results

In the following, we present definitions of IBM's single-qubit gates used in the experiments [27].

Gate	Definition
P	Applies a phase of $e^{i\theta}$
RZ	Rotates the qubit state around the z-axis by the given angle.
RX	Rotates the qubit state around the x-axis by the given angle.
RY	Rotates the qubit state around the y-axis by the given angle.
$\sqrt{x}$	Creates an equal superposition state if the qubit is in the state $|0\rangle$, but with a different relative phase.
$\sqrt{x}^{\dagger}$	Inverse of the $\sqrt{x}$ gate.
Y	The Pauli Y gate.
U	Rotates the qubit state around the three-axis by the given angles.

TABLE II. Definition of single-qubit gates.

Appendix B: Algorithm

The algorithm produces different quantum circuits to design experiments that use cross-talk produced by QG to launch a row hammer attack in order to flip a qubit state as much as possible.

Algorithm 1: Factory

Input: center=72 extraSets= 0
1 **Function** getNodes(*node*):
2   **return** adjacent nodes

3 **Function** getNodesCombination(*lst1, lst2*):
4   lstNode=[];
5   **for** *a in lst1* **do**
6   save in lstNode the bidirectional connection among the qubits on the same row;
7   **for** *b in lst2* **do**
8   save in lstNode the bidirectional connection among the qubits of the two rows

9   **return** lstNode or list with the bidirectional connection between the rows' centre and adjacent qubits

10 **Function** makeCircuitAndMeasure(*centerMeasure,cycles,*
11 *methodName*):
12   channels = getNodes(centerMeasure);
    // Depending on methodName, build the circuit on the channels
13   **else if** *methodName == cx* **then**
14   **for** _ *in range(0,cycles)* **do**
15   **for** *x in getNodesCombination([channels])* **do**
16   fn(qreg_q[x[0]], qreg_q[x[1]])
17   qc.barrier(*qreg_q[0:qNumber])

18   qc.measure(qreg_q[centerMeasure], creg_c[0]);
19   **return** circuit

20 circuit1 = makeCircuitAndMeasure(center,1+extraSets,'sx');
21 expLst.append(transpile(circuit1, backend, optimization_level=0));
Output: CSV file

Appendix C: Flipping rates of single-qubits

The following tables show the flipping rates corresponding to each single-qubit gate. The Output 0 and Output 1 indicate changes in the measurement outcomes based on whether a bit flip did not occur or occur respectively. Hence, this implies that the experimental results are stable and reliable for using cross-talk to implement the row hammer attack. It can be seen that the rate of bit flip is low for the Kyiv QC as compared to the Osaka QC.

Experiment	Output 0 %	Output 1 %
Precision(109)	94.7125	5.2875
-p(109-1000) 6	94.48	5.52
-rz(109-1000) 6	94.6575	5.3425
-rx(109-1000) 6	93.1325	6.8675
-ry(109-1000) 6	93.325	6.675
$-\sqrt{x}$(109-1000) 6	93.905	6.095
$-\sqrt{x}^{\dagger}$(109-1000) 6	94.085	5.915
-y(109-1000) 6	94.06	5.94
-u(109-1000) 6	93.4025	6.5975

TABLE III. Kyiv single-qubit experimental results.

Experiment	Output 0 %	Output 1 %
Precision(34)	83.3525	16.6475
p(34-1000) 6	82.965	17.035
rz(34-1000) 6	17.1025	82.8975
rx(34-1000) 6	24.1825	75.8175
ry(34-1000) 6	75.9025	24.0975
$\sqrt{x}$(34-1000) 6	21.4125	78.5875
$\sqrt{x}^{\dagger}$(34-1000) 6	20.8825	79.1175
y(34-1000) 6	79.24	20.76
u(34-1000) 6	75.9675	24.0325

TABLE IV. Osaka single-qubit experimental results.

Appendix D: Kyiv and Brisbane results

The results for QCs Kyiv and Brisbane are shown here. These figures represent the flipping rates for different configurations of the C-Not gate. The flipping of the target qubit from $|0\rangle$ to $|1\rangle$ and vice versa is considered to be successful when the observed flipping rate is greater than $^2/_3$ of the total number of experiments performed.
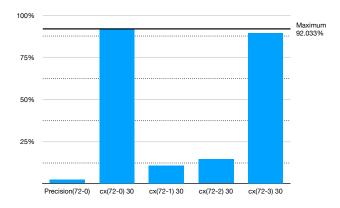

FIG. 9. Brisbane A: Flipping $|0\rangle$ to $|1\rangle$. Successful rate of 40,000 experiments on qubit flipping using different C-Not gates setups on a specific IBM QC.

FIG. 10. Brisbane B: Flipping $|0\rangle$ to $|1\rangle$. Successful rate of 40,000 experiments on qubit flipping using different C-Not gates setups on a specific IBM QC.
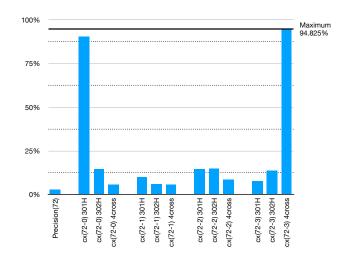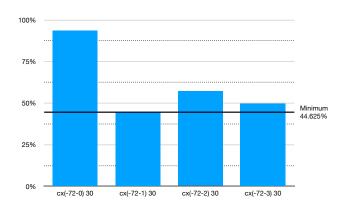

FIG. 11. Brisbane: Flipping $|1\rangle$ to $|0\rangle$. Successful rate of 40,000 experiments on qubit flipping using different C-Not gates setups on a specific IBM QC.
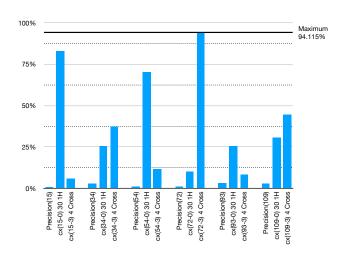

FIG. 12. Brisbane: Flipping $|0\rangle$ to $|1\rangle$ on different centres. Successful rate of 40,000 experiments on qubit flipping using different C-Not gates setups on a specific IBM QC.
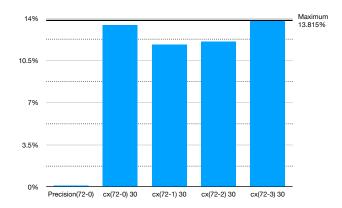
FIG. 13. Kyiv A: Flipping $|0\rangle$ to $|1\rangle$. Successful rate of 40,000 experiments on qubit flipping using different C-Not gates setups on a specific IBM QC.

FIG. 14. Kyiv B: Flipping $|0\rangle$ to $|1\rangle$. Successful rate of 40,000 experiments on qubit flipping using different C-Not gates setups on a specific IBM QC.
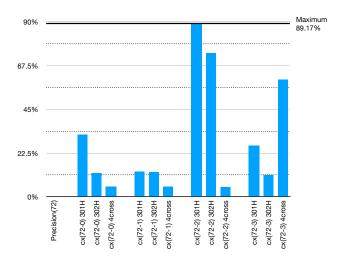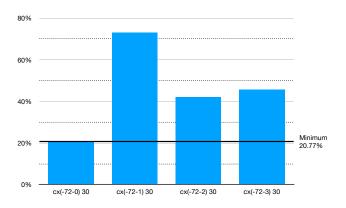

FIG. 15. Kyiv: Flipping $|1\rangle$ to $|0\rangle$. Successful rate of 40,000 experiments on qubit flipping using different C-Not gates setups on a specific IBM QC.

FIG. 16. Kyiv: Flipping $|0\rangle$ to $|1\rangle$ states on different centres. Successful rate of 40,000 experiments on qubit flipping using different C-Not gates setups on a specific IBM QC.

FIG. 17. Kyiv: Flipping $|1\rangle$ to $|0\rangle$ states on different centres. Successful rate of 40,000 experiments on qubit flipping using different C-Not gates setups on a specific IBM QC.

Appendix E: Cramér's V

Cramér's V is an effect size measurement for the chi-square test of independence. It measures how strongly two categorical fields are associated [28], and is defined as

$$\text{Cramér's V} = \sqrt{\frac{\chi^2}{n \times \min(c-1,\ r-1)}},$$

where

- χ^2 is the Chi-square statistic,
- n: is the total sample size,
- r: is the number of rows in the data,
- c: is the number of columns in the data.

This measure has the following meaning

Effect size (ES)	Interpretation
ES = 0	No association among the fields.
ES $\leq$ 0.2	The result is weak. Although the result is statistically significant.
0.2 < ES $\leq$ 0.6	The fields are moderately associated.
ES > 0.6	The fields are strongly associated.
ES = 1	There is a perfect association among the fields.

TABLE V. Cramér's V interpretation

Experiment	Output 0 frequency	Output 1 frequency	Total	Expected$_0$	Expected$_1$	$\left[\frac{(O-E)^2}{E}\right]_0$	$\left[\frac{(O-E)^2}{E}\right]_1$	Label	Result
Precision(72)	38925	1075	40000	27444.41	12555.58	4802.57	10497.62	χ^2	334515.18
cx(-72-0) 30	2644	37356	40000	27444.41	12555.58	22411.13	48986.98	min (c-1,r-1)	1
cx(72-0) 301H	3912	36088	40000	27444.41	12555.58	20178.03	44105.81	n	680000
cx(72-0) 302H	34282	5718	40000	27444.41	12555.58	1703.53	3723.64	Cramér's V	0.70
cx(72-0) 4cross	37728	2272	40000	27444.41	12555.58	3853.32	8422.71		
cx(-72-1) 30	22150	17850	40000	27444.41	12555.58	1021.36	2232.53		
cx(72-1) 301H	36013	3987	40000	27444.41	12555.58	2675.25	5847.65		
cx(72-1) 302H	37547	2453	40000	27444.41	12555.58	3718.87	8128.83		
cx(72-1) 4cross	37795	2205	40000	27444.41	12555.58	3903.69	8532.82		
cx(-72-2) 30	17153	22847	40000	27444.41	12555.58	3859.18	8435.53		
cx(72-2) 301H	34160	5840	40000	27444.41	12555.58	1643.28	3591.95		
cx(72-2) 302H	34086	5914	40000	27444.41	12555.58	1607.27	3513.23		
cx(72-2) 4cross	36576	3424	40000	27444.41	12555.58	3038.35	6641.33		
cx(-72-3) 30	20036	19964	40000	27444.41	12555.58	1999.84	4371.32		
cx(72-3) 301H	36972	3028	40000	27444.41	12555.58	3307.59	7229.84		
cx(72-3) 302H	34506	5494	40000	27444.41	12555.58	1816.98	3971.62		
cx(72-3) 4cross	2070	37930	40000	27444.41	12555.58	23460.54	51280.81		
Total	466555	213445	680000						

TABLE VI. Cramér's V Brisbane shows a 0.7 value, which means that these fields, the use of C-Not gates and the cross-talk measured by the qubit flipping are strongly associated.

* fernando.almaguerangeles@phdstud.ug.edu.pl
† pedro.dieguez@ug.edu.pl
‡ akshata.shenoy@ug.edu.pl
§ marcin.pawlowski@ug.edu.pl

[1] John Preskill. Quantum Computing in the NISQ era and beyond. *Quantum*, 2:79, August 2018.

[2] Muhammad AbuGhanem and Hichem Eleuch. Nisq computers: a path to quantum supremacy. *IEEE Access*, 2024.

[3] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando GSL Brandao, David A Buell, et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.

[4] Christopher Portmann and Renato Renner. Security in quantum cryptography. *Reviews of Modern Physics*, 94(2):025008, 2022.

[5] Vincenzo Lordi and John M Nichol. Advances and opportunities in materials science for scalable quantum computing. *MRS Bulletin*, 46:589–595, 2021.

[6] Bela Bauer, Sergey Bravyi, Mario Motta, and Garnet Kin-Lic Chan. Quantum algorithms for quantum chemistry and quantum materials science. *Chemical reviews*, 120(22):12685–12717, 2020.

[7] Soohyun Park and Joongheon Kim. Trends in quantum reinforcement learning: State-of-the-arts and the road ahead. *ETRI Journal*, 46(5):748–758, 2024.

[8] Joseph F Fitzsimons. Private quantum computation: an introduction to blind quantum computing and related protocols. *npj Quantum Information*, 3(1):23, 2017.

[9] Vittorio Giovannetti, Lorenzo Maccone, Tomoyuki Morimae, and Terry G. Rudolph. Efficient universal blind quantum computation. *Phys. Rev. Lett.*, 111:230501, Dec 2013.

[10] Atul Mantri, Carlos A. Pérez-Delgado, and Joseph F. Fitzsimons. Optimal blind quantum computation. *Phys. Rev. Lett.*, 111:230502, Dec 2013.

[11] Spyridon Samonas and David Coss. The cia strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, 10(3), 2014.

[12] Bryan C Ward, Richard Skowyra, Samuel Jero, Nathan Burow, Hamed Okhravi, Howard Shrobe, and Roger

Khazan. Security considerations for next-generation operating systems for cyber-physical systems. In *1st International Workshop on Next-Generation Operating Systems for Cyber-Physical Systems (NGOSCPS)*, 2019.

[13] Elisabetta Biasin and Erik Kamenjašević. Cybersecurity of medical devices: new challenges arising from the ai act and nis 2 directive proposals. *International Cybersecurity Law Review*, 3(1):163–180, May 2022.

[14] Juan M Pino, Jennifer M Dreiling, Caroline Figgatt, John P Gaebler, Steven A Moses, CH Baldwin, M Foss-Feig, D Hayes, K Mayer, C Ryan-Anderson, et al. Demonstration of the qccd trapped-ion quantum computer architecture. *arXiv preprint arXiv:2003.01293*, pages 28–29, 2020.

[15] David Abraham, Jerry Chow, Antonio Corcoles, Mary Rothwell, George Keefe, Jay Gambetta, Matthias Steffen, and Quantum Computing Team. Cross-talk in superconducting transmon quantum computing architecture. In *APS March Meeting Abstracts*, volume 2013, pages W27–003, 2013.

[16] Ch Piltz, Th Sriarunothai, AF Varón, and Ch Wunderlich. A trapped-ion-based quantum byte with 10- 5 next-neighbour cross-talk. *Nature communications*, 5(1):4679, 2014.

[17] Mohan Sarovar, Timothy Proctor, Kenneth Rudinger, Kevin Young, Erik Nielsen, and Robin Blume-Kohout. Detecting crosstalk errors in quantum information processors. *Quantum*, 4:321, 2020.

[18] Yoongu Kim, Ross Daly, Jeremie Kim, Chris Fallin, Ji Hye Lee, Donghyuk Lee, Chris Wilkerson, Konrad Lai, and Onur Mutlu. Flipping bits in memory without accessing them: An experimental study of dram disturbance errors. *ACM SIGARCH Computer Architecture News*, 42(3):361–372, 2014.

[19] Dayeon Kim, Hyungdong Park, Inguk Yeo, Youn Kyu Lee, Youngmin Kim, Hyung-Min Lee, and Kon-Woo Kwon. Rowhammer attacks in dynamic random-access memory and defense methods. *Sensors*, 24(2):592, 2024.

[20] cve.org. https://www.cve.org/CVERecord?id=CVE-2015-0565. [Accessed 18-03-2025].

[21] cve.org. https://www.cve.org/CVERecord?id=CVE-2016-6728. [Accessed 18-03-2025].

[22] Introducing Half-Double: New hammering technique for DRAM Rowhammer bug — security.googleblog.com. https://security.googleblog.com/2021/05/introducing-half-double-new-hammering.html. [Accessed 18-03-2025].

[23] Daniel Gruss, Clémentine Maurice, and Stefan Mangard. Rowhammer.js: A remote software-induced fault attack in javascript, 2015.

[24] Sampler (latest version) | IBM Quantum Documentation — docs.quantum.ibm.com. https://docs.quantum.ibm.com/api/qiskit/qiskit.primitives.Sampler. [Accessed 18-03-2025].

[25] Hello world | IBM Quantum Documentation — docs.quantum.ibm.com. https://docs.quantum.ibm.com/guides/hello-world, 2024. [Accessed 29-10-2024].

[26] Exact and noisy simulation with Qiskit Aer primitives | IBM Quantum Documentation — docs.quantum.ibm.com. https://docs.quantum.ibm.com/guides/simulate-with-qiskit-aer, 2024. [Accessed 29-10-2024].

[27] library (latest version) | IBM Quantum Documentation — docs.quantum.ibm.com. https://docs.quantum.ibm.com/api/qiskit/circuit_library. [Accessed 17-03-2025].

[28] Cramér's v — ibm.com. https://www.ibm.com/docs/en/cognos-analytics/11.1.0?topic=terms-cramrs-v. [Accessed 11-03-2025].