

A Systematic Methodology to Compute the Quantum Vulnerability Factors for Quantum Circuits

Original

A Systematic Methodology to Compute the Quantum Vulnerability Factors for Quantum Circuits / Oliveira, Daniel; Giusto, Edoardo; Baheri, Betis; Guan, Qiang; Montrucchio, Bartolomeo; Rech, Paolo. - In: IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING. - ISSN 1545-5971. - (2024), pp. 1-15. [10.1109/TDSC.2023.3313934]

Availability:

This version is available at: 11583/2986648 since: 2024-03-07T14:59:22Z

Publisher:

IEEE

Published

DOI:10.1109/TDSC.2023.3313934

Terms of use:

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright

(Article begins on next page)

A Systematic Methodology to Compute the Quantum Vulnerability Factors for Quantum Circuits

Daniel Oliveira[†], Edoardo Giusto^{*}, Betis Baheri[‡], Qiang Guan[‡], Bartolomeo Montrucchio^{*}, Paolo Rech[§]

[†]Department of Informatics, Federal University of Paraná (UFPR), Curitiba, Brazil
dagoliveira@inf.ufpr.br

^{*}DAUIN, Politecnico di Torino, Torino, Italy

{eduardo.giusto, bartolomeo.montrucchio}@polito.it

[‡]Department of Computer Science, Kent State University, Kent, USA

{bbaheri, qguan}@kent.edu

[§]Department of Industrial Engineering, Università di Trento, Italy

paolo.rech@unitn.it

Abstract—Quantum computing is one of the most promising technology advances of the latest years. Qubits are highly sensitive to noise, which can make the output useless. Lately, it has been shown that superconducting qubits are extremely susceptible to external sources of faults, such as ionizing radiation. When adopted in large scale, radiation-induced errors are expected to become a serious challenge for qubits reliability. We propose an evaluation of the impact of transient faults in the execution of quantum circuits on superconducting chips. Inspired by the Architectural and Program Vulnerability Factors, widely used for classical computation, we propose the Quantum Vulnerability Factor (QVF) to measure the impact of qubit corruption on the circuit output. We model faults, and design a fault injector, based on the latest studies on real machines and radiation experiments. We report the finding of more than 388,000,000 fault injections, considering single and double faults, on three algorithms, identifying the faults and qubits that are more likely to impact the output. We give guidelines on how to map the qubits in real devices to reduce the output error and to reduce the probability of having a radiation-induced corruption modifying the output. Finally, we compare simulations with experiments on physical quantum computers.

Index Terms—Quantum computing, Fault injection, Reliability evaluation, QVF metric.



1 INTRODUCTION

Quantum computing is quickly moving from being a conceptual solution to physics problems to an extremely efficient and promising computing architecture for critical applications, such as big data [1], machine learning [2], chemistry [3], and drug development [4], just to name a few.

The turning point that made the intriguing theory of quantum computing a promising computing paradigm was the achievement of sufficiently fault tolerant qubits to allow the computation of small, yet crucial, circuits [5], [6]. The reliability challenge of qubits is intrinsic in the unpredictability of quantum mechanics (the state of qubits can be randomly changed) and the sensitivity of qubits to external perturbations. As technology improved, major industries developed their prototypes of quantum machines and today offer researchers access to several quantum computers, such as IBM, D-Wave, Rigetti, Pasqal, and quantum circuit simulators [7], [8]. The billions of dollars investments of industries, research centers, and government agencies in quantum computing are encouraging the development of large-scale quantum computers as well as the training of quantum programmers and hardware designers.

The production of stable qubits is allowing us to increase the size of quantum circuits, is pushing the adoption of quantum computing in large scale, but, unfortunately, is

also arising novel challenges in the reliability of quantum circuits that cannot be underestimated. In fact, recently pioneer works have demonstrated that, besides noise, it is necessary to harden superconducting qubits also from external radiation [9], [10], [11], [12] as the interaction of ionizing particles significantly reduces the fault tolerance of qubits [13], [14], [15]. Trapped-ion qubits are found to be robust to low-dose low-energy radiation [16], but no data is available for heavier particles, yet. As most studies focus on superconducting qubits we will consider this technology as case study. Nevertheless, the concepts we introduce, the fault injection framework we design, and the impact of the results we present are independent on the qubit technology, once the fault model is defined. Already being one of the challenges for today's classical computing systems, then, ionizing radiation is expected to be a major issue also for future quantum (super) computers [10], [12]. Actually, as qubits have a higher sensitivity to external perturbation than CMOS transistors, quantum computers might be even more susceptible to ionizing radiation than classical computers. Recent studies showed that qubits can be affected by light particles, such as muons [15] or even infrared light [17], that do not have sufficient energy to significantly impact CMOS behavior.

Despite the fact that quantum computers are not yet fully available in a large scale of qubits, understanding and mitigating the radiation-induced faults is not premature. Recent discoveries have urged substantial reductions in operational error rates and further research into the mitigation of error mechanisms such as high-energy particles [10], [12]. The research community has been focused in making operative qubits, reducing their noise, neglecting other critical reliability challenges, as the one posed by ionizing particles. We cannot risk vanishing the efforts in producing stable quantum computers for realizing then, once adopted in the field, that the radiation-induced error rate is too high and still have not yet fully understood fault propagation.

In this paper, we aim at anticipating the need for a formal metric and providing researchers and developers with practical tools to evaluate the reliability of quantum circuits to transient faults. We investigate the effect on the quantum output of faults affecting each qubit of the circuit. Taking inspiration from the Architectural and Program Vulnerability Factors (AVF [18] and PVF [19]), which are the two most widely used metrics to measure the reliability of a device or code, we define the *Quantum Vulnerability Factor* (QVF) as an indicator of the vulnerability of the circuit to faults. A circuit with a low value of QVF is less vulnerable to faults than a circuit with a high QVF. Similarly to AVF and PVF, and for the same reasons, we do not investigate the probability for the fault to occur, but we rather assume that the fault occurred and track its propagation. The fault occurrence probability and fault generation mechanisms study is extremely interesting as it allows us to estimate the fault rate of a system. However, to implement effective hardening solutions, the circuit/code designer or the architect need to identify the resources that, once corrupted, are more likely to impact the output correctness so to quickly understand the vulnerabilities of the system and eventually take proper countermeasures. This applies to classical hardware resources (AVF), code portions (PVF), and, as we show in this paper, also to qubits and quantum circuits (QVF).

The main contributions of our work are:

- Based on the latest studies, we define how to model radiation-induced faults in superconducting qubits. Qubits do not have a binary value, thus, simply flipping a bit is not sufficient to model a fault. The status of a qubit is described by polar coordinates on the Bloch sphere (see Figure 1), and any modification to its value can be represented as a shift in one or both angles of the representation. We inject different phase shifts of different magnitudes to identify which phase shift is more critical and to highlight any possible correlation between the magnitude of the shift and the impact on the output.
- We design a quantum fault injector built on top of Qiskit that can also run on real quantum machines. We inject a fault by introducing a U gate in the target qubit. For each qubit, we inject up to 312 state changes in several positions of the circuit. The fault injector, the circuits, and the whole fault injection campaign are publicly available [20], [21].
- To study the fault impact in the output probabilities we introduce the QVF metric, based on the Michelson

Contrast, that quantifies how much the fault in a qubit reduces the confidence of the result.

- We provide a detailed QVF evaluation, identifying the quantum circuits and the qubits in each circuit that are more likely to be corrupted and quantifying the amplitude of the fault that is sufficient to corrupt the output.

The rest of the paper is organized as follows. To define, show a practical application, and prove the importance of QVF in understanding the reliability of quantum circuits, we give, in Section 2, some background information about quantum computing and radiation effects in qubits. Then, in Section 3, we formalize the Quantum Vulnerability Factor metric and, in Section 4, we describe the fault model we inject and the fault injection framework we used to evaluate the QVF of qubits and quantum circuits. The obtained results are presented in Section 5, in Section 6 we discuss the impact of our findings, and Section 7 concludes the paper.

2 BACKGROUND AND RELATED WORK

In this Section, we give a background about quantum computing and the impact of ionizing radiation on qubits, which is essential to understand and appreciate the contribution of our paper. As there is not yet sufficient data on radiation effects on trapped-ion qubits (besides the low-dose test documented in [16]), we will focus the discussion on superconducting materials. Nonetheless, the concepts we introduce, the fault injection framework we design, and the impact of the results we present are independent on the qubit technology, once the fault model is defined. The details provided in this Section serve as a solid background to justify the chosen fault model.

2.1 State of the art in quantum computing systems

Even though the physical implementation of quantum computing technology covers more than 20 different approaches from Quantum dot computers to Nuclear magnetic resonance quantum computers, the most popular and successful attempts in this domain are Trapped Ion and Superconducting quantum computers, the latter being capable of running the majority of quantum algorithms.

As the biggest quantum computing service provider, the IBM quantum system includes 24 quantum computers available, with qubit capacity ranging from 5 to 127, with public access through API services provided by IBM. Among the 21 available quantum computers, three types of quantum processors are implemented: Canary, Falcon, and Hummingbird. Each quantum processor model uses different qubit topologies, which may greatly impact the machine quantum noise and quantum errors on computation results [22].

Quantum programs are expressed as quantum circuits, in which a set of quantum gates are sequentially applied to the initial qubits, and produce a probabilistic output across all combinations of the classical bits. These quantum circuits will be mapped to qubits from Noisy Intermediate-Scale Quantum (NISQ) machines based on the topological connectivity of the qubits and the availability of the supported gate types. Programming on different quantum

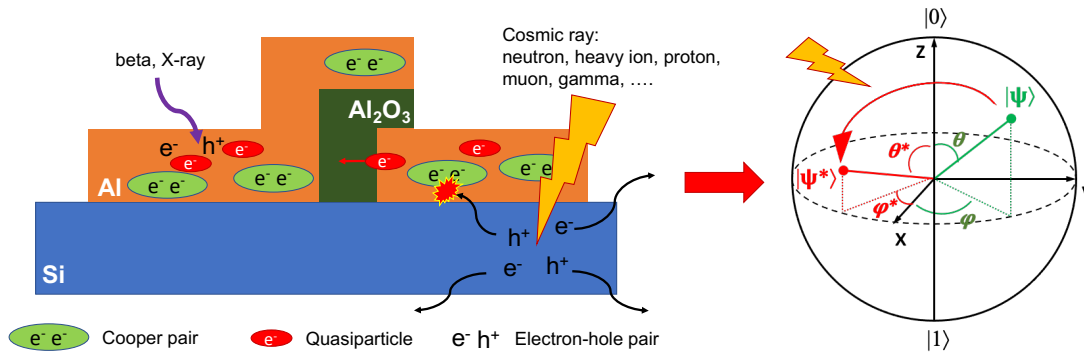


Fig. 1: Simplified effect of the impact of ionizing radiation with superconducting qubit material (on the left, adapted from [14]) and its consequences on the qubit state (on the right, adapted from [15]). The charge deposited by radiation in Silicon or Aluminum generates electron-hole pairs that induce a non-equilibrium and breaks the Cooper pair, producing quasiparticles. The excess of quasiparticles excites the qubit. The excitement is logically translated into phase(s) shift(s) and a state change from the expected $|\Psi\rangle$ to the corrupted $|\Psi^*\rangle$.

platforms and quantum simulators has been constrained by the quantum compilers supported by different systems. Qiskit [7] and QASM [23] are generally supported by IBM quantum machines. Both Qiskit and QASM are imperative programming languages and designed machine-independent. In our experiments, we focus on studying the IBM quantum machines and running benchmark quantum programs in Qiskit.

In spite of the fact that the qubit capacity of quantum computers is ever-increasing, the performance of quantum computers is bounded by the quantum noise, which is greatly reducing the accuracy and performance of the IBM quantum computers [24]. Quantum noise can be categorized into operation errors and retention (coherence) errors [25]. A qubit can retain data (position) only for a limited time (coherence time). Retention errors are categorized into two types, T1 and T2 errors [26]. A qubit in a high energy state $|1\rangle$ naturally decays to lower energy state $|0\rangle$, the time associated with this decay is called spin-lattice coherence time (T1). The spin-spin relaxation process (T2) indicates the time for a qubit to get affected by the external environment or by the interaction with other qubits. Depending on the material used in NISQ machines, individual qubits have a time range for T1 and T2 that has improved in the last decade from 1 nano-second to 100 micro-seconds [27].

Hardware-based noise reduction is still under investigation by IBM-Q, which is working to improve the environment and qubit design by updating the quantum processor and even using new isolation techniques. In the IBM-Q system One, IBM tried to isolate the interaction with noise and qubits by separating the quantum computer from the surrounding environment. However, the hardware approach is only one of the dimensions to consider, depending on the circuit depth and noise on gates and measurements, the level of quantum noise affecting the results can change in a certain range.

Quantum Error Correction (QEC) has been fundamental to reach Fault Tolerant Quantum Computers (FTQC). QEC is designed to protect a qubit from noise, at the extremely high cost of requiring from 5x to 9x larger circuits.

As the qubits are more and more stable and reach an

operative dimension, other critical reliability aspects need to be considered. Unfortunately, the strategies adopted to reduce intrinsic quantum machine noise, which are already implemented in frameworks like qiskit, are not the *panacea* for all possible faults mechanisms. In fact, as particles impacts are stochastic and unpredictable, unlike noise, typical QEC is inefficient in handling radiation-induced and correlated faults [13], [14], [15]. To reach FTQC we need to design better QEC, and the first step is the understanding of faults impact and their propagation, which is the main scope of this paper.

2.2 Radiation effects in superconducting qubits

It is known from extensive studies in traditional computing systems that the impact of radiation with the computing device can induce transient current spikes that propagate through the architecture, possibly modifying the executed operations output [28]. These physical events are referred to as *radiation-induced faults*. Preliminary and inspiring works show that ionizing radiation induces faults in superconducting qubits [13], [14], [15], [17] and, once employed in large scale, radiation fault tolerance is expected to be the next big challenge for quantum (super-) computers [9], [10], [11], [12]. The available Quantum Error Correction (QEC) approaches, such as the Shor error correcting code [29] or surface codes [30], are effective under the assumption that physical (redundant) qubits are not affected by correlated multiple events. Unfortunately, such an assumption does not apply to radiation-induced faults since the deposited charge spreads in the quantum chip Silicon substrate, affecting multiple physical qubits [31]. These uncorrelated multiple qubits corruption make QEC ineffective.

As shown in Figure 1, adapted from [14] and [15], the impact of ionizing radiation on the qubit superconducting materials increases the amount of hole-electron pairs in the Aluminum thin-film and Silicon substrate. Heavy particles are more likely to interact with Silicon (*Al* is transparent to neutrons), while other sources of radiation (β , X-rays) with Aluminum. While there is still no quantitative measurement of the radiation-induced fault rate in quantum circuits, it is known that the additional charge deposited by the

impinging particle induces a non-equilibrium that leads to Cooper pairs break and, thus, quasiparticles generation [14], [15]. The resulting excitement modifies the state of the qubit, possibly changing its state (i.e., it induces ϕ and/or θ phase shift) as shown with simulations [15] and experimentally validated [10]. While for CMOS a fault is generated only if the charge is higher than the critical charge [28], on a qubit any excitement modifies the state, inducing a phase shift with a magnitude that depends on the deposited charge [32]. It has also been shown that if, and only if, the deposited charge is sufficiently high, the qubit collapses [14]. The physical interaction of the particle with the qubit, then, modifies its state. Such a modification can be propagated through the quantum circuit that is using the struck qubit(s), eventually corrupting the output.

Terrestrial neutrons and heavy ions, which are today the most critical source of faults for Silicon-based classical computing devices [28], generate a large amount of electrons-holes pairs in the Silicon substrate. The energy spectrum of neutrons ranges from meV to GeV, the lower energy ones being exponentially more common. Unfortunately, the frailty of qubits makes it not unlikely for low energy neutrons and lighter particles, such as muons (almost harmless for CMOS technology [33]), to induce a sufficient perturbation in the qubit to generate a fault [15].

An interesting difference between particles is that γ -rays, β , X-rays have a constant and accumulative effect while the neutrons, heavy ions, and muons impact is stochastic and transient. In other words, γ -rays, β , and X-rays exposure constantly deposits a little amount of charge, until inducing a fault or qubit collapsing [14] (or a permanent CMOS transistor malfunction [34]). Neutrons and heavy ions strikes are random (the neutrons flux at sea level is $\sim 13n/(cm^2 \times h)$ [35]) and the impact with the device material produces a transient charge that can lead to a fault.

Unfortunately, while a thin shielding could be sufficient to drastically reduce the number of X-rays reaching the qubit, as mentioned in [14], the shielding for neutrons and heavy ions is impractical (meters of concrete or lead) and for muons is basically impossible as the qubit should be placed in deep underground caves [15]. As a result, as known for traditional computing devices, it is impossible to shield qubits from transient faults. We must find effective and efficient solutions to deal with the unavoidable transient faults in qubits.

2.3 Contribution

Unlike previous work on quantum fault tolerance, we target transient fault reliability, which is the next challenge in the quest of large scale quantum computers. We focus on the effects of faults in quantum computation rather than investigating the physical fault mechanisms. As in the AVF or PVF measurement, we assume that the fault occurred independently of the cause, and understand its effect on the quantum circuit output. While recently a preliminary fault injector to track noise propagation was presented [36], there is still no fault injector to track transient fault propagation in quantum circuits. In this paper, we introduce a novel fault injector integrated with Qiskit and that can be used also in real quantum machines. Additionally, we formalize

a new metric, the Quantum Vulnerability Factor, based on Michelson Contrast, to ease the analysis of quantum circuit reliability.

We aim at practically estimating the reliability of a circuit and at identifying the qubits in a circuit that, once affected, are more likely to induce a negative impact on the circuit correctness. Such information is highly valuable as it allows us to map the circuit qubits to physical qubits in the most reliable way and to predict the effects of faults in the quantum computation.

3 QUANTUM VULNERABILITY FACTOR

In this Section we present the Quantum Vulnerability Factor (QVF) metric, to better understand the reliability and fault propagation in quantum circuits. QVF is inspired by the Architectural/Program Vulnerability Factors (AVF/PVF), that measure the probability for a fault in traditional computing devices/codes to affect computation.

As we will discuss, while there are already some metrics available to quantify the quality of quantum circuit outputs, none of these metrics provide sufficient information on the fault propagation effect.

The output of a quantum circuit is a set of states, each with a different probability. The state(s) with the higher probability is(are) considered the output. Most works use the Probability of Successful Trial (PST) metric when evaluating the reliability and correctness of a quantum circuit output [37], [38], [39], [40]. PST considers only the probability of the correct state and is defined by Equation 1.

$$PST = \frac{\text{Number of successful trials}}{\text{Total number of trials}} \quad (1)$$

The PST metric on its own cannot quantify nor qualify if a circuit is reliable and cannot give overall information about the state probability distribution we are investigating. To use PST one needs to specify a threshold to define when a circuit can be considered reliable. For instance, one could argue that circuits with $PST > 0.68$ are sufficiently good, and a circuit with a $PST = 0.5$ fails the reliability assessment. Unfortunately, defining a threshold, such as 1-sigma, masks the details of the fault effects on the output state distribution and may deem reliable circuits as unreliable. As we show later in this Section, using the example in Figure 2, values close to the threshold are identified as correct but can be highly susceptible to external perturbations, such as radiation. While increasing the PST may indeed improve the reliability, this increase can also affect the overall probability distribution and thus increase the probability of a single incorrect state.

The Inference Strength (IST) metric has been introduced to identify whether the quantum circuit execution was successful or not, by calculating the strength and comparing it with a threshold [41]. However, to have a full reliability understanding it is fundamental to understand how the fault impacts the output, independently of the output selection.

To understand the reliability of a circuit, and consequently the impact of a fault on the output correctness (i.e., on the output probability distribution), we extend the PST metric as follows. First, we compute the Michelson Contrast [42]. We use the Michelson Contrast since it naturally

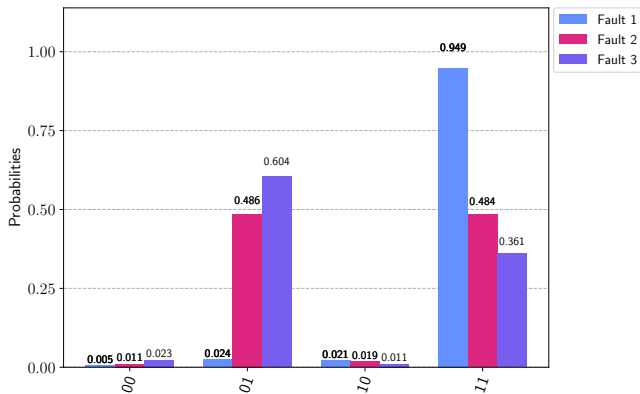


Fig. 2: The probability distribution for three fault injections in a 2-qubit Grover circuit. The correct state is 11, and QVF resulting from the injection of fault 1, 2, and 3 is 0.03, 0.50, and 0.63 respectively.

measures how distinguishable one object is from others using color, luminance, or, as in our specific case, the probability of each output state. In other words, the Michelson Contrast defines how confidently (i.e., how distinguished) one can select the correct state among all states in the output. Some studies employ other metrics, such as *KL-divergence* or *Hellinger fidelity* [41]. These metrics however require the whole output probability distribution sample state to be computed, since this calculation depends on a comparison between the two probabilities of the same state. In the next few years, quantum computers will have thousands or even millions of qubits, making it impractical (or impossible) to completely sample their probability distribution. This is the reason why QVF employs the Michelson Contrast, which makes it highly scalable and able to cope also with future large quantum computers.

$$Contrast = \frac{P(A) - P(B)}{P(A) + P(B)} \quad (2)$$

Equation 2 shows the contrast computation, where $P(A)$ is the probability of the correct state (i.e., the expected state in a fault-free execution), and $P(B)$ is the highest probability among any of the incorrect states (i.e., the most probable incorrect state). Please note that PST is precisely $P(A)$ in Equation 2 of our contrast metric [38], but we include $P(B)$ to consider also the overall probability distribution.

It is also important to point out that the contrast metric is not limited to circuits with a single correct state; the extension for circuits with multiple correct-state outputs can be easily performed by aggregating the probabilities of all correct states into $P(A)$.

Since it is possible for a circuit to produce $P(A) < P(B)$ (e.g., due to technology, noise, or external factors such as radiation-induced faults), the contrast range is $[-1, 1]$. To shift the range to $[0, 1]$ and to have lower values indicating a more reliable configuration (as for AVF and PVF), the QVF is calculated as shown in Equation 3:

$$QVF = 1 - (Contrast + 1)/2 \quad (3)$$

By this definition, QVF values close to zero indicate a clear contrast between the correct state and the incorrect

ones, with the correct state presenting the highest probability. In other words, the probability to have the expected output state is very high compared to the other states. QVF values around 0.5 present the correct state and at least one incorrect state with similar probabilities, which makes the identification of correct states dubious. Finally, values close to one represent the worst case in a probability distribution where the correct states are not even as high as the incorrect ones.

While both PST and QVF, in some cases, can both identify output corruptions, QVF also provides additional and essential information about the fault impact in the output. In fact, QVF, by considering the closeness of the most probable and second most probable output configuration, estimates the impact of the fault in the output reliability. The closer the two configurations are (higher QVF), the more likely the selection of the wrong configuration becomes. QVF, unlike PST, can also identify those faults that reach the output modifying the output probability distribution without changing the configuration that has the higher probability.

To better illustrate the QVF calculation and meaning, Figure 2 shows the probability distribution for a 2-qubits Grover circuit in which we perform 3 fault injections. The correct state is 11 and the most probable incorrect state is 01 for all three faults. Then, $P(A) = P(11)$ and $P(B) = P(01)$ for all three fault injection. The QVF results for each circuit are as follows:

- Fault 1: $P(A) = 0.949$, $P(B) = 0.024$, $QVF = 0.03$
- Fault 2: $P(A) = 0.484$, $P(B) = 0.486$, $QVF = 0.50$
- Fault 3: $P(A) = 0.361$, $P(B) = 0.604$, $QVF = 0.63$

The circuit has a very low QVF for the first fault (0.03), as evident from Figure 2, indicating that the correct state 11, with a probability of about 95%, can be reliably selected. The second fault has a QVF of about 0.50, which indicates that it is not possible to reliably select the correct state (11 and 01 states are almost equally probable). Finally, the third fault has a high QVF of 0.63, indicating that the incorrect state 01 is more likely to be selected as the output, which can lead to errors. As a result, we can state that fault 1 (low QVF) is not very critical, while fault 2 and mostly fault 3 should be strictly avoided as they drastically change the output state distribution. It is worth noting that PST would have identified the outcome of fault 1 as correct and both faults 2 and 3 as wrong. However, no information about the impact on the output state distribution would have been given.

To further illustrate the weakness of PST with an arbitrary threshold in the evaluation we are proposing, let us consider a fault in a 5-qubit circuit with the probability distribution shown in Figure 3. The correct state of this circuit is 00100 and the probability for this state is about 50%, while the probability for any incorrect state is at most 1.76% (i.e., all of the 31 remaining states have a similar probability). Thus, the output of this faulty circuit results in a PST of 0.5, rejecting that circuit as unreliable (depending on the threshold defined). However, the QVF is 0.03 indicating that the correct state can be confidently identified, even if one defines a strict threshold. This is evident in Figure 3, since the state 00100 is the only state with non-negligible probability, and the remaining states can be easily identified as noise.

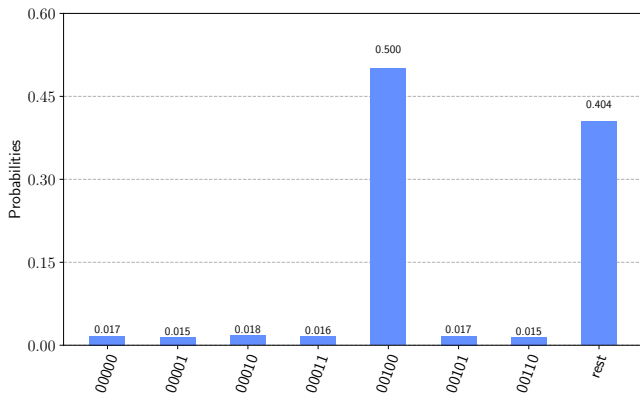


Fig. 3: The probability distribution for a fault in a 5-qubit circuit (the rest is the sum of the probabilities of the remaining states). The correct state is 00100, resulting in $PST = 0.5$ (probably considered wrong) and $QVF = 0.03$ (fault has a minor effect in the output).

To measure the QVF as well as the impact of faults, we designed a fault injector for the quantum circuit described in Section 4. We inject faults in each qubit and track the effect of each injection in the output. When comparing the QVF of a fault-free circuit to a faulty one, we can observe how much a circuit or its individual qubits are sensitive to faults. While PST serves as an innovative metric for gauging the effectiveness of quantum circuits, its adaptability for fault injection techniques falls short. As equation 3 pointed out, factors such as technology, noise, and external influences can drastically alter the final probability distribution. Hence, the QVF metric was formulated to encapsulate the comprehensive results of fault injections. In a previous example, we demonstrated the effect of each fault injection. However, its application is not restricted to a specific circuit outcome; it can be universally applied to any circuit(s).

4 FAULT INJECTION FRAMEWORK

In this Section, we first describe how we model the fault from the available knowledge on qubit sensitivity to radiation. Then, we describe the fault injection framework we developed.

4.1 Fault model

To have a realistic study of the radiation-induced fault propagation in quantum circuits we first need to define the fault model to inject, i.e., how radiation modifies the qubit state. We model the faults to inject based on the latest discoveries on qubits radiation vulnerability, that have shown that even a small deposition of charge from an impinging particle reduces the coherence time and can lead to unexpected modifications of the qubit state [10], [14], [15], [32]. This physical fault is then propagated through the visible states and we track its effect on the circuit output.

In a classical computer, a fault is generated when the impinging particle deposits enough charge to change the binary state of a transistor [28]. While a traditional bit can be either 1 or 0, the qubit state is associated with the θ and ϕ coordinates that represent its amplitude and phase. In a

qubit, then, the impact of the impinging particle is logically reflected as a state change that can be represented with ϕ and/or θ phase(s) shift(s), independently of the source (see Figure 1).

A θ phase shift changes the 0-1 probability in the qubit, while a ϕ phase shift changes its orientation. Both shifts can impact the correctness of the execution, and it is part of our contribution to identify which phase shift in which qubit is more critical for a quantum circuit. It has been mathematically proved [32] and showed with simulations [43] that a higher charge deposition induces a bigger phase shift. As the charge deposition of the radiation-induced impact depends on the energy of the impinging particle (which goes from meV to GeV [28]) and on the distance between the impact location and the qubit, the resulting phase shift magnitude can be largely variable. Thus, we inject and track the propagation of shifts of different magnitudes as well as combinations of shifts ($\theta + \phi$) to correlate the circuit behavior to a wide spectrum of effects. As discussed in Section 4, the amplitude and direction of the injected phase shift is a parameter in our fault injection framework.

A major event or a cumulative charge deposition, as shown in [14] for X-rays, can also lead the qubit to collapse. In such an event, the qubit ceases to operate, there would be no reason to measure its QVF and there would be no other practical solution than re-executing the whole circuit. As the vast majority of neutrons have low energy and the cumulative effect of X-rays can be easily shielded [14], radiation-induced qubit collapses are expected to be less likely than phase shifts.

4.2 Noise

The quantum circuit execution is known to be noisy, even in the absence of faults. Faults will happen on top of the already noisy execution. Based on the information provided e.g., by IBM, it is possible to have a clear and detailed characterization of the noise in each physical qubit [44].

To have a full understanding of the effects of faults in the quantum circuit execution, our fault injector can be executed with three different scenarios. (1) Simulation without external noise, ideal but unrealistic environment. (2) Simulation of a physical machine, using the IBM-Q noise model to create a realistic environment based on actual quantum computers. (3) Injection over the circuit execution on a physical IBM-Q machine. In this paper, we only present data obtained with scenario (2) and (3) since scenario (1) cannot be achieved in the real world. Considering the noise, executed or modeled after a physical machine, helps us to understand how each qubit and fault severity can change the state probability distribution. It is worth noting that it is possible for a fault to attenuate the noise effect by changing ϕ or θ in opposite directions, improving the circuit reliability.

4.3 Fault injector

Our fault injector is built on the open-source and well-documented Qiskit framework [7]. The fault injector operates over a Qiskit's *QuantumCircuit* object to generate new circuits with fault(s) injected. This operation is performed automatically, and the new faulty circuits can be transpiled

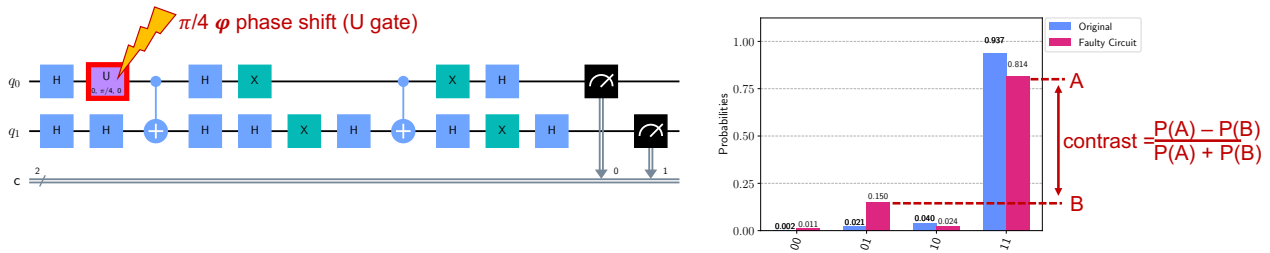


Fig. 4: Example of fault injection in the Grover circuit (left) and QVF calculation (right). A θ shift of $\frac{\pi}{4}$ is injected in q_0 after the first H-gate. The fault modifies the output probabilities distribution, shown to the right, from the blue one to the red one. As shown in Equation 3, QVF is calculated using the Michelson Contrast, where A is the probability of the expected (fault-free) output (11 in this case) and B is the highest probability among the wrong outputs (01).

and executed just as one would execute a regular *Quantum-Circuit*. Thus, we can execute the faulty circuits in physical IBM-Q machines as well as simulators, or even export them as QASM files to load and execute the circuits on different systems. Moreover, we set up our *QuantumCircuit* objects to be exactly like the circuits transpiled to the physical IBM-Q machines we target (e.g., using only available gates supported by the physical machines). Then, injecting faults before or after the transpilation phase will produce the same results.

To model the injected fault, we used Qiskit's most generic gate, the U gate, to effectively simulate every possible phase shift. The U gate can be described as:

$$U(\theta, \phi, \lambda) = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -e^{i\lambda} \sin\left(\frac{\theta}{2}\right) \\ e^{i\phi} \sin\left(\frac{\theta}{2}\right) & e^{i(\phi+\lambda)} \cos\left(\frac{\theta}{2}\right) \end{bmatrix} \quad (4)$$

which receives three parameters:

- ϕ is the angle defined in the XY plane of the Bloch sphere (a rotation angle on the Z axis);
- θ is the angle defined in the plane that includes the Z axis and the vector representing the generic quantum state $|\psi\rangle$;
- λ is also a rotation on the Z axis.

The parameters for the U gate have been thus selected:

- $\phi = [0, 2\pi]$ every 15° ;
- $\theta = [0, \pi]$ every 15° ;
- $\lambda = 0$

This angle combination results in 312 possible configurations of the U gate (injections) for each position in the quantum circuit.

Furthermore, by injecting faults, our fault injector is not modifying the qubit mapping but simply simulating the radiation effect. For this work, we consider only the default mapping policy, but one can use our framework to study the reliability impact of distinct mapping policies. Moreover, the time to execute, or simulate, a faulty circuit is about the same time the fault-free circuit takes, since we only include a single gate. Still, for deep or large circuits, due to the high number of qubits or gates, the time required to inject faults in all possible injection sites could be prohibitively high. While in this paper we present *exhaustive* fault injection results, when the circuit complexity is too high it is possible to use QuFI to perform a *statistical* fault injection, as commonly performed for complex traditional devices and algorithms [45].

It is worth noting that our fault injector is also able to inject (correlated) multiple faults, as these events have already been observed in multi-qubits circuits [15]. For the sake of simplicity, this paper considers only single and double fault injection scenarios.

4.3.1 Single fault injection

For the purpose of this study, we inject faults after each gate in the original circuit, simulating faults in each one of the circuit operations (see Figure 4). The single qubit QVF is calculated averaging the QVF obtained by all the injection in all the possible fault sites (gates). This is a common strategy adopted in transient fault evaluation, since the radiation-induced event is stochastic in time and can occur in any instant during the circuit calculation. We still maintain the QVF of each single fault site and, thus, filtering the injection data it is possible to understand the QVF of each possible fault site, identifying the most critical locations. Fault positions, as well as the fault model, can be easily modified to better correspond to reality as the understanding of quantum computer's reliability progresses.

Figure 4 illustrates a single fault injection in a 2-qubit Grover circuit. The fault is injected in qubit q_0 after the first Hadamard gate with a θ phase shift of $\frac{\pi}{4}$. The probability distributions of the original and faulty circuit are plotted on the right. The correct state is 11 and the $P(A)$ (i.e., the PST) is 0.937 for the original circuit and 0.814 for the faulty one. To compute the contrast in Equation 2 and the QVF in Equation 3, we also need $P(B)$. For the original circuit $P(B) = P(10) = 0.040$, while for the faulty one $P(B) = P(01) = 0.150$. Then, the QVF is 0.04 for the original and 0.16 for the faulty circuit.

4.3.2 Double fault injection

Due to the significance of these phenomena, we cannot disregard the possibility of concurrent radiation-induced corruption of multiple qubits [14].

The charge deposited by a single impinging particle is able to spread rapidly on the substrate of the chip, producing a phase shift in two (or more) qubits that are physically close to each other (i.e., neighboring qubits).

For our analysis, we limit the injections to neighboring qubit pairs. The amplitude of the phase shift, as mentioned, depends on the amount of deposited charge. The qubit that is closer to the particle impact will then experience a bigger phase shift. In our injection we consider, for the fault in the

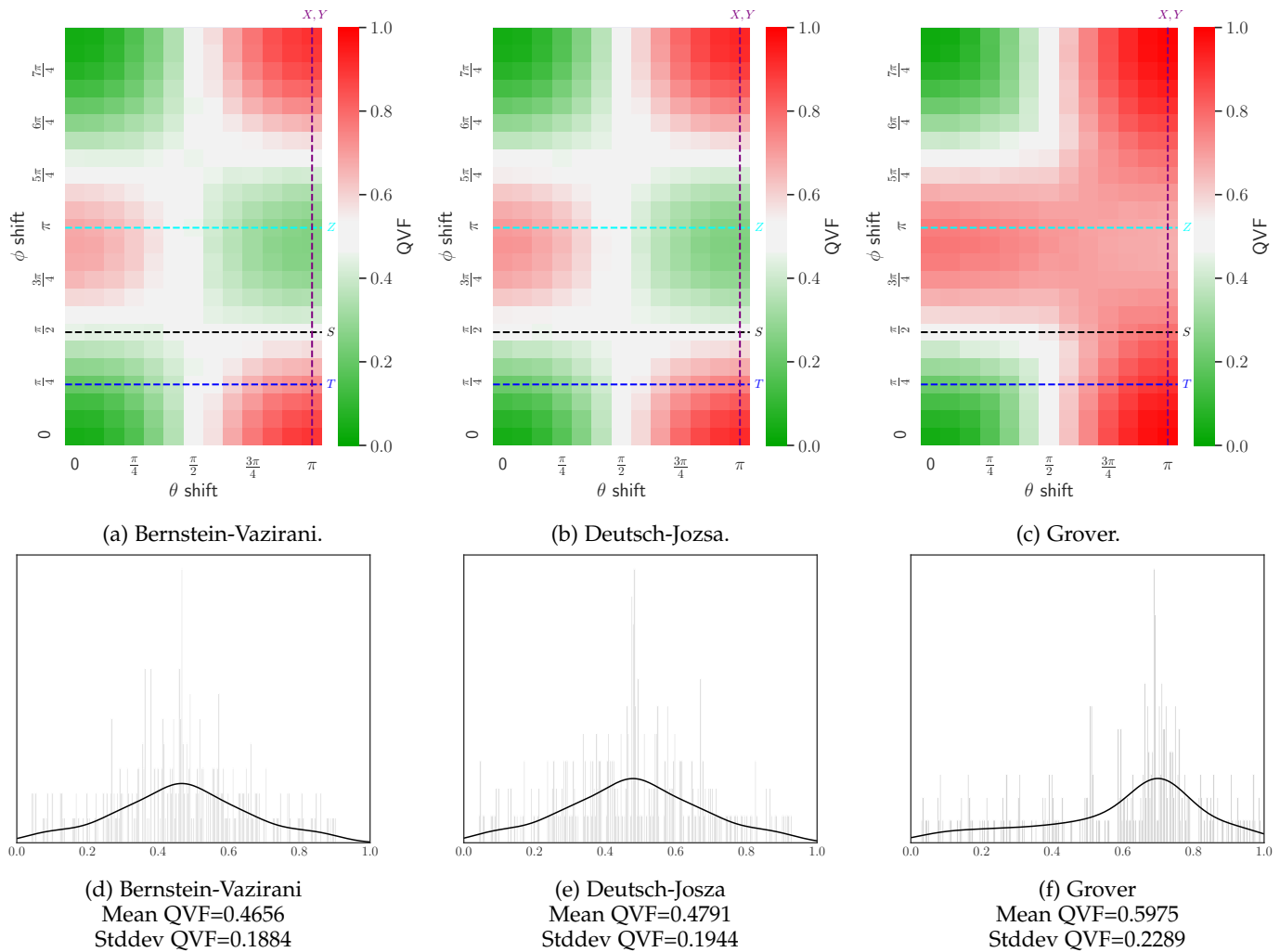


Fig. 5: (a, b, c) QVF heatmaps for the different circuits for different values of ϕ and/or θ shifts. The green color indicates a low QVF (the correct state can be confidently selected), the red color indicates a higher QVF (an incorrect output is more likely to be selected), and the white color indicates a dubious output (i.e., correct and incorrect states have about the same probability). The plot also shows dotted lines corresponding to the effect of common quantum gates (X, Y, S, T, Z) in order to provide a quick reference for the fault effect in the qubit. (d, e, f) Histograms of the QVF distribution of the three considered circuits.

neighbor qubit (farther from the impact), a smaller phase shift magnitude than the one of the first qubit (closer to the particle impact). The second fault, then, is characterized by a magnitude going from 0 to the one of the first fault, in any possible direction.

5 EXPERIMENTAL RESULTS

In this Section, to illustrate and highlight the impact of QVF, we present the results obtained by injecting faults in three widely known and most used quantum circuits: **Deutsch-Jozsa** [46] (4 qubits) is the first algorithm that showed that Quantum Computer could be faster than classical computers, **Bernstein-Vazirani** [47] (4 qubits) is an extension of Deutsch-Jozsa that identifies a string encoded in a function, and **Grover** [1] (2 qubits) speeds up unstructured searches by performing just $O(\sqrt{N})$ evaluations, which is the fastest a quantum algorithm can perform [48].

We first inject single faults in all three circuits and then consider also double faults in Deutsch-Jozsa and Grover circuits. We show data of 388, 763, 648 total injections. The original codes of circuits, data of faults injected, and output results are publicly available [20], [21].

5.1 Single fault results

As a radiation-induced fault can cause a ϕ and/or θ phase shift of various amplitudes, for each fault location we inject ϕ and/or θ angles with 15° steps (i.e., $\frac{\pi}{12}$) for a range of $\phi = [0, \pi]$ and $\theta = [0, 2\pi)$. For each fault we execute the circuit 1, 024 times to obtain the probability distribution. Bernstein-Vazirani has 13 possible fault positions, thus requiring 4, 056 distinct faults and a total of 4, 153, 344 executions. Grover and Deutsch-Jozsa have 18 fault positions each, which leads to 5, 616 distinct faults and 5, 750, 784 executions. Thus, for the three circuits, we perform a fault injection campaign of 15, 654, 912 total executions.

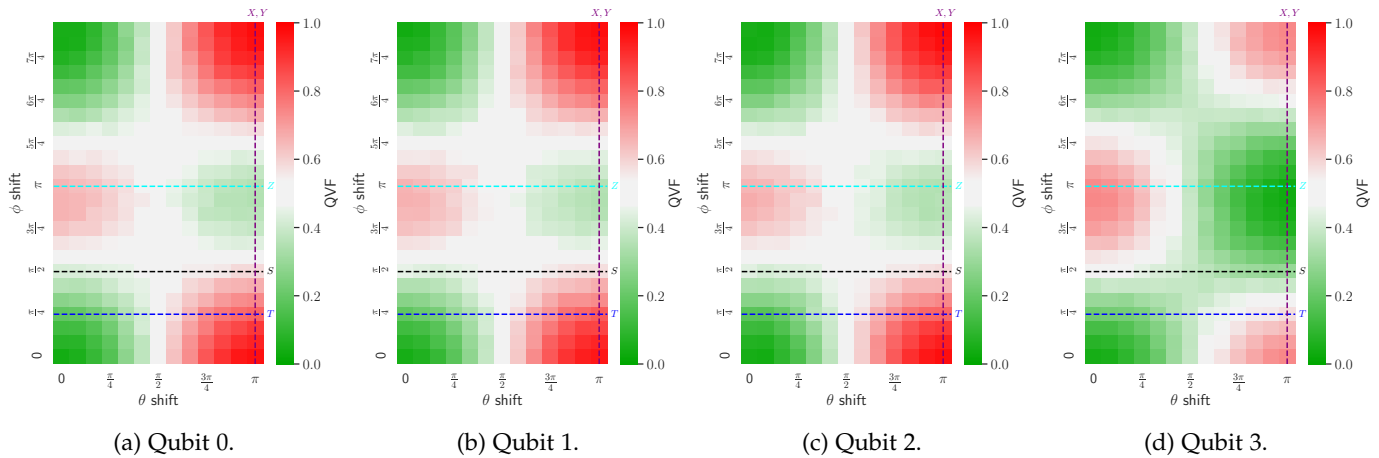


Fig. 6: QVF, per qubit, for Bernstein-Vazirani circuit for different values of ϕ and θ . The green color indicates that the correct state can be confidently selected, the red color an incorrect one will be selected, and the white color produces a dubious output (i.e., correct and incorrect states have about the same probability).

Unlike classical computing, we need to consider a great number of possible configurations for each fault location, and each injection can have various impacts on the circuit output. We plot different graphs to visually appreciate the fault impact in a quantum circuit output. We start the QVF analysis by showing, in Figure 5, the heatmap of the QVF for the considered quantum circuits. We plot, for each circuit, the QVF computed for each fault (i.e., the injected ϕ and/or θ shifts). Each spot (ϕ, θ) represents the QVF mean for all possible fault injections (qubit and position inside a qubit) for that specific (ϕ, θ) phase shift. To have a more direct reference of the effect of faults in the qubit state, in Figure 5 we also superposed colored lines corresponding to the phase shifts that would be imposed by common quantum gates (X, Y, S, T, Z).

Green colors in Figure 5 ($\text{QVF} < 0.45$) mean the circuit still produces the correct output as the most likely one. White colors ($0.45 < \text{QVF} < 0.55$) means that the fault causes the output to be dubious (i.e., the correct output cannot be confidently selected). Finally, red colors ($\text{QVF} > 0.55$) means that the fault effect is so high to produce an incorrect output as the most likely, leading to errors. These colors are used to ease the visualization and can be changed when an acceptable threshold for QVF is defined.

Let us consider, in Figure 5, the $(\phi = 0, \theta = 0)$ spot. This square represents the QVF computed for the fault-free, yet noisy, execution of the circuits. The value for this square is not solid green (i.e., $\text{QVF} = 0$), since the circuit itself has its own imperfections due to noise. Interestingly, we found that, in some rare cases ($\sim 3\%$), faults seem to improve the circuit QVF compared to the fault-free (but noisy) execution. This apparently happens because the injected fault compensates for the intrinsic noise effect, making the output state distribution closer to the ideal case. Further investigations would be required to better understand this behavior. The fact that a fault improves the output quality should not surprise, as it has been observed in probabilistic classical - such as artificial neural networks (despite with much lower probability) [49] - and quantum computation applications [50].

By fixing the injected ϕ shift to 0 (we are keeping for ϕ the same value of the noisy, but fault-free, execution) and moving to the right in Figure 5 we can study the effect of injecting a fault with increasing θ from 0 to π (without shifting ϕ). In other words, we are gradually modifying the 0-1 probability in the qubit without changing the ϕ phase. As shown in Figure 5, increasing θ keeping the fault-free ϕ increases the QVF and, thus, makes the circuit highly unreliable. It is worth noting that a $\frac{\pi}{2}$ shift in θ is the point where the output becomes dubious, and that is exactly the angle (90°) where the direction starts to flip in the Bloch sphere. For shifts greater than $\frac{\pi}{2}$ the 0-1 probability of the qubit is effectively changed and an incorrect state becomes the most likely one.

A similar trend is observed for ϕ when θ is not shifted, however, the QVF is not as severely impacted as for θ , resulting in lower QVF values but still higher than 0.55 (red colors). Thus, a shift in θ (i.e., a shift in the 0-1 state probability) is indeed more critical than a shift in ϕ . While this seems not surprising, please note that for Bernstein-Vazirani and Deutsch-Jozsa, the combination of a θ and ϕ shift (e.g., $(\phi = \pi, \theta = \pi)$) has a beneficial effect on the QVF. Thus, this combination seems to compensate for the shift resulting in still acceptable QVFs (green colors). In contrast, Grover has a different response to the combination of a θ and ϕ shift, and it is not sufficient to produce acceptable QVFs. For instance, QVF mean for $(\phi = \pi, \theta = \pi)$ is 0.254224, 0.249150, and 0.666607 for Bernstein-Vazirani, Deutsch-Jozsa, and Grover, respectively.

An additional interesting insight is that Figure 5 is almost symmetric on ϕ with respect to π . This is justified as moving towards 2π on the Bloch sphere as we pass π we move closer to the original position of ϕ .

Figure 5 can also be used to have a first comparison of the reliability of circuits. The higher the number of red spots, the higher the number of faults that can corrupt the circuit output. Figure 5 (d, e, f) are in fact depicting the histograms of QVF for the three algorithms, showing also the QVF mean value and standard deviation. Grover algorithm presents, in the QVF map of all faults, a mean value of 0.59, which

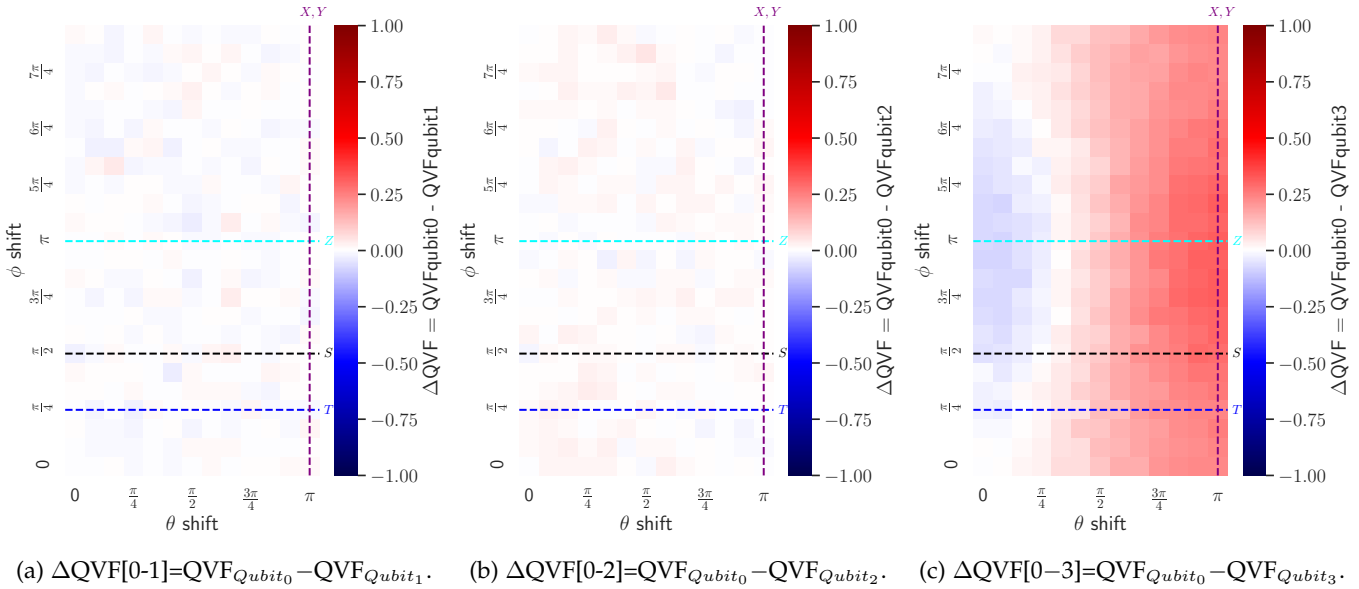


Fig. 7: ΔQVF for Bernstein-Vazirani circuit between different qubits.

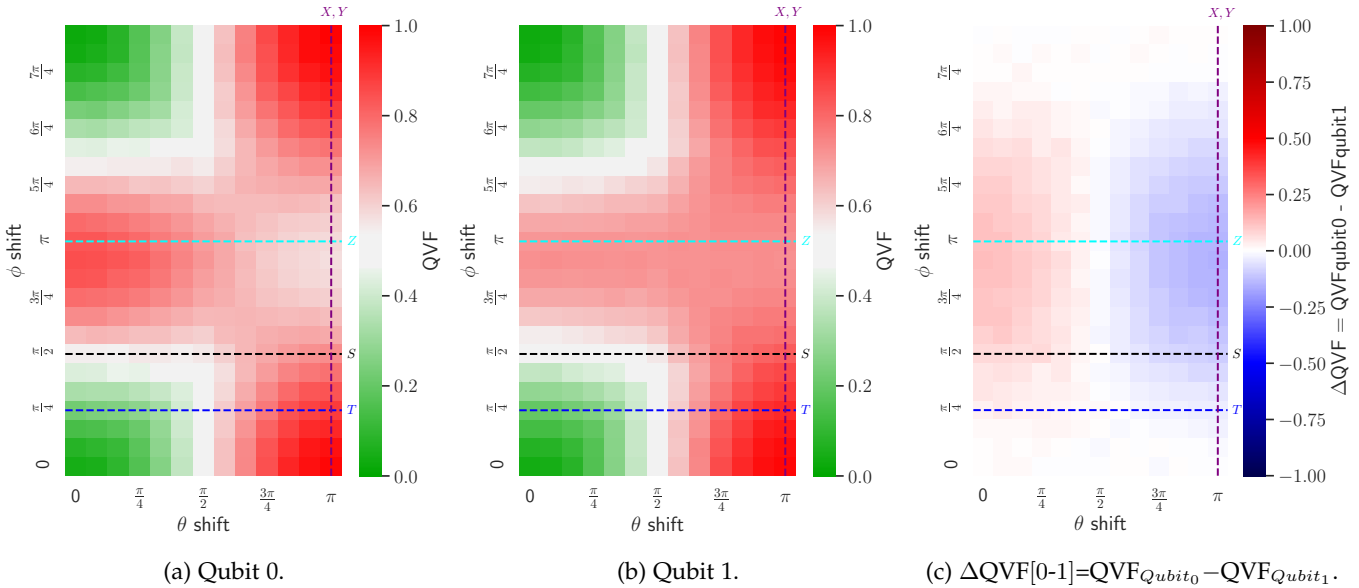


Fig. 8: QVF for Grover circuit for each qubit and the ΔQVF between them.

means that the circuit grants more probability to the wrong result than to the right one (0.5 is the automatic threshold). The other two algorithms are much better, with both a lower mean value (lower than 0.5) and a reduced standard deviation. Histograms can provide a method that does not require human intervention and that could be applied to a large number of random circuits and/or specific faults. Histogram plotting and other image processing techniques can be applied to the whole image or on a subsection of it.

Additionally, Figure 5 gives an indication of the faults that are more critical for a given circuit. For instance, any shift with $\theta > \frac{\pi}{2}$ and/or $\frac{\pi}{2} < \phi < \frac{5\pi}{4}$ is critical for Grover. However, this is not the case for Bernstein-Vazirani nor Deutsch-Jozsa, indicating that the fault criticality is circuit-dependent and cannot be assumed a priori. The amplitude of the phase shift resulting from the particles hit depends

on the amount of energy deposited by the impinging particle [32], [43]. Clearly, the deposited charge depends on the particle energy and the location of the hit (the closer the particle hit the higher the portion of energy that will reach the qubit). Since the position and energy of the impinging particles are stochastic, in Figure 5 we assume each phase shift to be equally probable. If in a specific application some energies are found to be more likely than others, thus requiring a different probability of a specific (ϕ, θ) probability to occur, we can normalize the QVF for each (ϕ, θ) probability and provide a more realistic comparison.

An insight we can derive from the QVF evaluation is the identification of the qubit(s) in a circuit that is more likely, if corrupted, to impact the output correctness. This is fundamental information as it allows us to focus the design and implementation of extra fault tolerance solutions where

they are more needed.

To better understand the impact of a fault depending on the faulty qubit, we plot, in Figure 6, the heatmap of QVF for each one of the four qubits of the Bernstein-Vazirani circuit (we do not plot the heatmap for the qubits of the other circuits for lack of space). These plots show that there are areas (ϕ and/or θ shift injections) that are more critical for circuit correctness than others. The plot for qubit 3, being lighter among the four qubits, implies that it is less likely for a fault in qubit 3 to impact the overall behavior of the circuit. In fact, the QVF mean for qubits 0 to 3 in ($\phi = \pi, \theta = \pi$) is, respectively, 0.348350, 0.347449, 0.357679, and 0.036119. This is justified by the fact that qubit 3 in Bernstein-Vazirani acts as an ancilla qubit (i.e., auxiliary qubit). As qubit 3 is not directly measured at the output, it has a lower QVF.

We can better understand the different vulnerabilities of qubits from the heatmaps in Figure 7, in which we plot, for the Bernstein-Vazirani circuit, the Δ QVF, i.e. the difference between the QVF of each pair of qubits. Please note that values higher than zero (red colors) indicate that the former qubit has a higher QVF, and thus a higher impact on the circuit output than the latter. Δ QVF lower than zero (blue colors) indicates the opposite, with the former qubit having a lower QVF, and thus better reliability than the latter. There is not much difference between qubit 0 and qubit 1 (Fig.7a) or between qubit 0 and qubit 2 (Fig.7b). The maximum Δ QVF for both cases is 0.048622 and the minimum -0.034 . However, there is definitely an appreciable difference between qubit 0 and qubit 3 (Fig.7c), for which the maximum Δ QVF is 0.317 and, for $\theta \geq \frac{\pi}{2}$, all values are higher than 0.127. In this case, qubit 0 performs worse than qubit 3 with an overall Δ QVF mean of 0.113, hence the prevailing red colors. Thus, as observed before, qubit 3 acts as an ancilla qubit and has a lower impact on the circuit.

Figure 8 shows the QVF for the two qubits in the Grover circuit and the delta between them. From these plots, it is possible to see that the two qubits have a mirrored performance with respect to $\theta = \frac{\pi}{2}$ and centered on $\phi = \pi$. This means that, starting from $\phi = \pi$ and $\theta = \frac{\pi}{2}$ and moving to the left, one qubit performs worse and the other better, while if we move to the right we have the opposite trend.

5.2 Double fault results

It is known that the interaction of a single particle with quantum devices can modify the state of multiple qubits [14]. As introduced in Section 4.3.2, for our double fault injection campaign, for each fault injected in the circuit (all possible combinations of ϕ and θ) we include an additional fault on a neighboring qubit. Considering the fact that charge from a particle strike spreads through the chip substrate, we expect this additional fault to be of a lesser magnitude with respect to the first one. The magnitude intervals for this additional injection are $[0, \phi_1]$ and $[0, \theta_1]$, where ϕ_1 and θ_1 are the angles of the first injected fault. Thus, we evaluate the impact of double faults injections in a 4-qubit Deutsch-Jozsa circuit (Figure 9) and in a 2-qubit Grover circuit (Figure 10). For the sake of space, we just plot two circuits as Deutsch-Jozsa and Bernstein-Vazirani have very similar behaviors. The complete data can be found in the public repository. We limit the first fault ϕ parameter

to $[0, \pi]$ since we observe results are symmetric on ϕ with respect to π (see Figure 5). Then, the chosen parameters results in 149,058 distinct double faults for Grover and 215,306 for Deutsch-Jozsa. We execute the distinct faults 1,024 times to obtain the probability distribution, resulting in 373,108,736 total executions.

Figures 9 and 10 depict first the single (a) and double (b) fault QVF heatmaps. Then, Δ QVFs (c) are shown to better quantify the impact of double faults for specific phase shifts, where red squares indicate an increased impact for double faults and blue squares a reduced impact. Finally, we present the QVF histogram distributions (d) for single and double faults, black and red lines respectively. The histograms clearly present how the overall QVF changes in the presence of double faults.

As shown in Figures 9a and 9b, the double fault injection has a greater impact on the QVF in the Deutsch-Jozsa circuit. In fact, Figure 9b shows that red zones in the lower-right and upper-left occupy a greater area. Moreover, faults around ($\theta = \pi, \phi = \pi$), acceptable for single fault, are now unacceptable with correlated faults. This is also highlighted by the Δ QVF in Figure 9c, where it is possible to see that the upper-right corner in red denotes an increased effect on the QVF due to the second fault injection. Another proof of the added effect of the double fault can be appreciated in Figure 9d. In this Figure, the histogram of double faults are significantly shifted toward higher (unacceptable) values of QVF. It is worth noting that the circuit sensitivity remains the same for small magnitude faults (i.e., lower-left corner), regardless of double or single faults.

The results for Grover circuit, shown in Figure 10, present a distinct behavior from the Deutsch-Jozsa ones. Figures 10a and 10b show that lower-right and upper-left areas of the graph are colored in a lighter red, indicating a reduced impact of the double fault with respect to the single fault injection. This behavior is also highlighted in Figure 10c, which displays an overall reduced (blue) impact for double faults. Furthermore, the QVF histograms for Grover, Figure 10d, show that the double fault QVF (red line) reaches a maximum of 0.77, while for the single injection the maximum value is 0.98. The high QVF values are shifted to a lower value, but still higher than 0.55, which is unacceptable. Similar to Deutsch-Jozsa, the sensitivity of small magnitude faults remains the same.

5.3 Real machine

Besides studying faults propagation using Qiskit simulator we have also injected faults, using our fault injector, on real quantum computers. Figure 11 shows the comparison between a simulation including the IBM-Q noise model and the physical IBM-Q Jakarta quantum machine. Due to time constraints for IBM physical machine reservations, we compare only four specific phase shift faults, which corresponds to basic gate operations (T, S, Z, and Y), in all possible fault positions for two circuits, Bernstein-Vazirani (Fig. 11a) and Grover (Fig. 11b). As we can see, there is only a small variation in QVF for both circuit and fault model types, which is expected since the noise is not static and may slightly change the state probability distribution. Thus, it is safe to assume that the results from simulation with noise

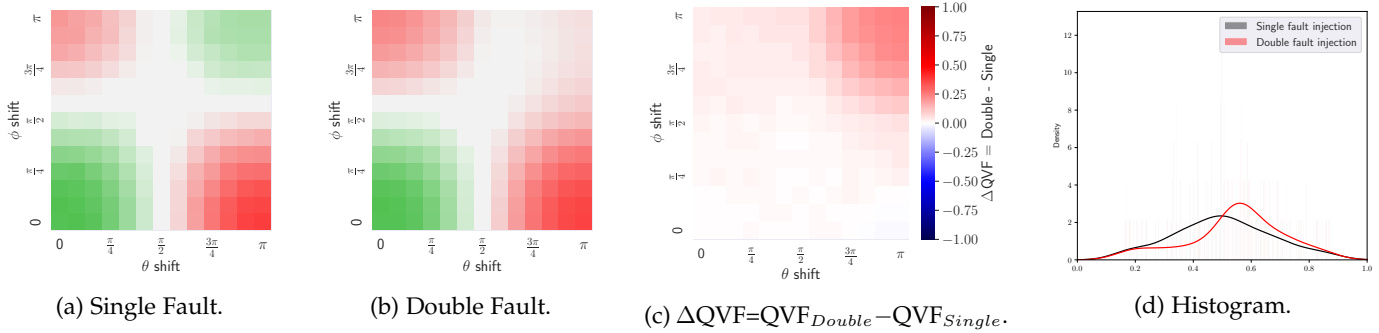


Fig. 9: Deutsch-Josza Algorithm: Single fault injection, double fault injection, Delta and Histogram.

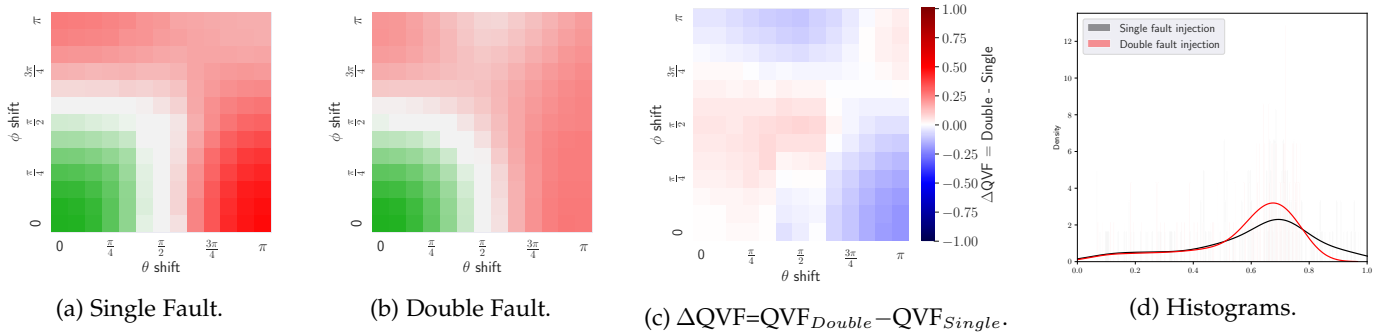


Fig. 10: Grover's Algorithm: Single fault injection, double fault injection, Delta and Histogram.

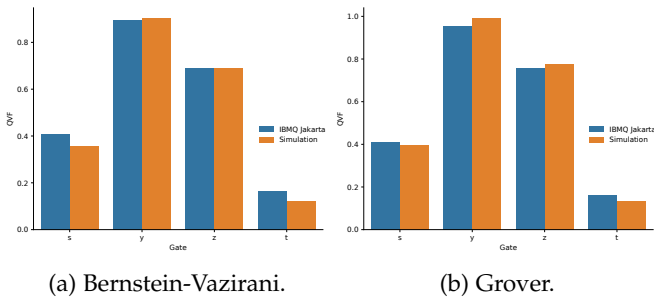


Fig. 11: QVF comparison between simulation using IBM-Q noise model and physical machine execution (IBMQ Jakarta).

models are precise enough to provide insights into physical machine executions.

6 DISCUSSION

In this Section we discuss the impact of our result and the potential of QVF for future development.

6.1 Threshold theorem and QVF

The quantum threshold theorem, as an analogue to von Neumann's threshold theorem for classical computers [51], states that it is possible to perform arbitrarily long quantum computations on a faulty quantum computer if the error probability per gate is below a certain threshold [52]. Recently, it has been also shown that the poly-logarithmic factor present in the standard threshold theorem is actually not needed and the factor can be reduced to a constant [53].

It appears that there are no physical implementation limitations for quantum computer realization, and this is an exciting result.

However, the threshold theorem needs some physically reasonable assumptions about the type of noise. Therefore, although the theorem demonstrates that a fault tolerance solution exists, such a solution needs to be implemented and is obviously engineered based on the expected error rate to avoid unnecessary overheads. Not considering radiation-induced faults risks to underestimate the error rate and to guarantee sufficient reliability it will be necessary to implement additional qubit fault tolerance [15]. Identifying the qubits that are more likely to require additional fault tolerance becomes then fundamental not to overestimate the redundancy or modification to apply to the circuit to make it sufficiently reliable. QVF can therefore be very useful in order to understand the impact of asynchronous faults on a circuit. This problem will become more and more important with the future increment of available qubit numbers and Michelson contrast's based QVF definition works well even when, due to a very large number of qubits, it is no longer possible to fully simulate the circuit or to run it for a number of times large enough to fully understand its probability distribution function; knowing the correct state probability and the most probable among the wrong states will suffice.

6.2 Qubit mapping

Multi-programming, much like in classical computation, is required to improve throughput and better utilize quantum hardware, especially in NISQ-era quantum chips [54]. However, mapping qubits into physical ones for single or multiple quantum circuits has also an impact on the overall

circuit reliability [40]. This impact is caused by the limited high fidelity quantum resources, cross-talk noise, and SWAP operations inserted due to the machine topology [39], [55]. The qubit QVF information we provide can be used also to improve such mappings, even in the absence of faults. To improve the quality of the circuit output, for instance, the qubits that are found more resilient to injections should be allocated to resources with lower fidelity. Recently proposed qubit mapping [39], [55] could further improve the circuit reliability by considering QVF as a mean to identify the qubits that are more likely, in the presence of noise, to affect the output correctness.

6.3 Large Circuits

For this work, using small circuits, we perform a fine-grain methodology considering every possible point of injection and a large number of possible fault magnitudes. This methodology is time-consuming and impractical for large circuits. It is worth noting that a similar fine-grain methodology is also impractical for classical algorithms, which cannot afford to inject faults in every point of injection. Thus, to perform a fault injection campaign in large circuits one need to adapt the methodology to an statistical approach. The statistical approach, similar to the classical methodology, consists in randomly select points of injection, carefully distributing faults after different types of gates. Then, this methodology will provide an approximation of the circuit reliability characteristics, which can be used to extract insights and improve its reliability.

7 CONCLUSIONS

In this paper, we have proposed the Quantum Vulnerability Factor (QVF) to better evaluate the sensitivity of qubits and quantum circuits to radiation-induced faults. The interaction with particles has been demonstrated to affect the qubit state and to be a serious problem for future quantum computers. By identifying the vulnerabilities to faults of circuits and qubits, the QVF provides useful information about the reliability characteristics of a circuit and identifies the qubits that, once corrupted, are more likely to affect the output state distribution.

Using a specially crafted fault injector, built on top of Qiskit, we have evaluated the QVF of all the qubits of three quantum circuits. We have modeled the faults as phase(s) shifts of different amplitude. Our evaluation also allows us to identify the kind of faults that are more critical for a circuit or qubit.

As quantum computers capability, the number of algorithms and applications, and the availability of quantum machines increases, we expect a growing interest in the radiation sensitivity of qubits. The QVF is then an effective metric to understand faults propagation and to identify the weaknesses of qubits and circuits. In the next future, quantum computers will have thousands of qubits. If we suppose to plot a QVF map for each qubit and to put all the maps one over the other like slices, we can, by means of techniques of volume rendering, explore the behavior of the whole computer, like by means of Nuclear Magnetic Resonance it is possible to explore the human body.

REFERENCES

- [1] L. K. Grover, "A fast quantum mechanical algorithm for database search," *arXiv e-prints*, pp. quant-ph/9605043, May 1996.
- [2] S. Lloyd, M. Mohseni, and P. Rebentrost, "Quantum algorithms for supervised and unsupervised machine learning," 2013.
- [3] A. Peruzzo *et al.*, "A variational eigensolver on a photonic quantum processor," *Nature Communications*, vol. 5, no. 1, p. 4213, 2014. [Online]. Available: <https://doi.org/10.1038/ncomms5213>
- [4] "Let's talk about quantum computing in drug discovery," *C&EN Global Enterprise*, vol. 98, no. 35, pp. 20–22, 09 2020. [Online]. Available: <https://doi.org/10.1021/cen-09835-feature2>
- [5] S. Bravyi *et al.*, "Correcting coherent errors with surface codes," *npj Quantum Information*, vol. 4, no. 1, p. 55, Oct 2018. [Online]. Available: <https://doi.org/10.1038/s41534-018-0106-y>
- [6] C. Chamberland *et al.*, "Triangular color codes on trivalent graphs with flag qubits," *New Journal of Physics*, vol. 22, no. 2, p. 023019, Feb 2020. [Online]. Available: <http://dx.doi.org/10.1088/1367-2630/ab68fd>
- [7] e. a. MD SAJJID ANIS, "Qiskit: An open-source framework for quantum computing," 2021.
- [8] A. Li *et al.*, *Density Matrix Quantum Circuit Simulation via the BSP Machine on Modern GPU Clusters*. IEEE Press, 2020.
- [9] A. D. Corcoles *et al.*, "Protecting superconducting qubits from radiation," *Applied Physics Letters*, vol. 99, no. 18, p. 181906, 2011. [Online]. Available: <https://doi.org/10.1063/1.3658630>
- [10] L. Cardani *et al.*, "Reducing the impact of radioactivity on quantum circuits in a deep-underground facility," *Nature Communications*, vol. 12, no. 1, p. 2733, 2021. [Online]. Available: <https://doi.org/10.1038/s41467-021-23032-z>
- [11] J. M. Martinis, "Saving superconducting quantum processors from decay and correlated errors generated by gamma and cosmic rays," *npj Quantum Information*, vol. 7, no. 1, p. 90, 2021. [Online]. Available: <https://doi.org/10.1038/s41534-021-00431-0>
- [12] Z. Chen *et al.*, "Exponential suppression of bit or phase errors with cyclic error correction," *Nature*, vol. 595, no. 7867, pp. 383–387, 2021. [Online]. Available: <https://doi.org/10.1038/s41586-021-03588-y>
- [13] L. Grünhaupt *et al.*, "Loss mechanisms and quasiparticle dynamics in superconducting microwave resonators made of thin-film granular aluminum," *Phys. Rev. Lett.*, vol. 121, p. 117001, Sep 2018. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.121.117001>
- [14] A. P. Vepsäläinen *et al.*, "Impact of ionizing radiation on superconducting qubit coherence," *Nature*, vol. 584, no. 7822, pp. 551–556, 2020. [Online]. Available: <https://doi.org/10.1038/s41586-020-2619-8>
- [15] C. D. Wilen *et al.*, "Correlated charge noise and relaxation errors in superconducting qubits," *Nature*, vol. 594, no. 7863, pp. 369–373, 2021. [Online]. Available: <https://doi.org/10.1038/s41586-021-03557-5>
- [16] J. Cui *et al.*, "Susceptibility of trapped-ion qubits to low-dose radiation sources," *Journal of Physics B: Atomic, Molecular and Optical Physics*, 2021. [Online]. Available: <http://iopscience.iop.org/article/10.1088/1361-6455/ac076c>
- [17] R. Barends *et al.*, "Minimizing quasiparticle generation from stray infrared light in superconducting quantum circuits," *Applied Physics Letters*, vol. 99, no. 11, p. 113507, 2011. [Online]. Available: <https://doi.org/10.1063/1.3638063>
- [18] S. S. Mukherjee *et al.*, "A Systematic Methodology to Compute the Architectural Vulnerability Factors for a High-Performance Microprocessor," in *Proceedings of the 36th Annual IEEE/ACM International Symposium on Microarchitecture*. Washington, DC, USA: IEEE Computer Society, 2003, pp. 29–.
- [19] V. Sridharan and D. R. Kaeli, "Eliminating microarchitectural dependency from architectural vulnerability," in *2009 IEEE 15th International Symposium on High Performance Computer Architecture*, 2009, pp. 117–128.
- [20] D. Oliveira *et al.*, "Dataset for a systematic methodology to compute the quantum vulnerability factors for quantum circuits," 2023. [Online]. Available: <https://dx.doi.org/10.21227/rnvb-6f83>
- [21] QuTAM, "Qufi - quantum fault injector public repository," <https://github.com/QuTAM/QuFI>.
- [22] L. Liu and X. Dou, "Qucloud: A new qubit mapping mechanism for multi-programming quantum computing in cloud environment," in *2021 IEEE International Symposium on High-Performance Computer Architecture (HPCA)*, 2021, pp. 167–178.

- [23] A. W. Cross *et al.*, "Openqasm 3: A broader and deeper quantum assembly language," 2021.
- [24] R. Harper, S. T. Flammia, and J. J. Wallman, "Efficient learning of quantum noise," *Nature Physics*, vol. 16, no. 12, pp. 1184–1188, Dec 2020. [Online]. Available: <https://doi.org/10.1038/s41567-020-0992-8>
- [25] D. Greenbaum and Z. Dutton, "Coherent errors in quantum error correction," in *APS March Meeting Abstracts*, ser. APS Meeting Abstracts, vol. 2017, Mar. 2017, p. R51.007.
- [26] X. Hu, R. de Sousa, and S. D. Sarma, "Decoherence and Dephasing in Spin-Based Solid State Quantum Computers," in *Foundations of Quantum Mechanics in the Light of New Technology ISQM-Tokyo '01*, Oct. 2002, pp. 3–11.
- [27] M. Kjaergaard *et al.*, "Superconducting qubits: Current state of play," *Annual Review of Condensed Matter Physics*, vol. 11, no. 1, p. 369–395, Mar 2020. [Online]. Available: <http://dx.doi.org/10.1146/annurev-conmatphys-031119-050605>
- [28] R. Baumann, "Soft errors in advanced computer systems," *IEEE Design Test of Computers*, vol. 22, no. 3, pp. 258–266, May 2005.
- [29] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A*, vol. 52, pp. R2493–R2496, Oct 1995. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.52.R2493>
- [30] S. B. Bravyi and A. Y. Kitaev, "Quantum codes on a lattice with boundary," *arXiv preprint quant-ph/9811052*, 1998.
- [31] M. McEwen *et al.*, "Resolving catastrophic error bursts from cosmic rays in large arrays of superconducting qubits," *Nature Physics*, vol. 18, no. 1, pp. 107–111, Jan. 2022. [Online]. Available: <https://doi.org/10.1038/s41567-021-01432-8>
- [32] G. Catelani *et al.*, "Relaxation and frequency shifts induced by quasiparticles in superconducting qubits," *Phys. Rev. B*, vol. 84, p. 064517, Aug 2011. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevB.84.064517>
- [33] B. D. Sierawski *et al.*, "Effects of scaling on muon-induced soft errors," in *2011 International Reliability Physics Symposium*, 2011, pp. 3C.3.1–3C.3.6.
- [34] T. Oldham and F. McLean, "Total ionizing dose effects in mos oxides and devices," *IEEE Transactions on Nuclear Science*, vol. 50, no. 3, pp. 483–499, 2003.
- [35] JEDEC, "Measurement and Reporting of Alpha Particle and Terrestrial Cosmic Ray-Induced Soft Errors in Semiconductor Devices," JEDEC Standard, Tech. Rep. JESD89A, 2006.
- [36] S. Resch *et al.*, "A day in the life of a quantum error," *IEEE Computer Architecture Letters*, vol. 20, no. 1, pp. 13–16, 2021.
- [37] S. S. Tannu and M. K. Qureshi, "Not all qubits are created equal: A case for variability-aware policies for nisq-era quantum computers," in *Proceedings of the Twenty-Fourth International Conference on Architectural Support for Programming Languages and Operating Systems*, ser. ASPLOS '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 987–999. [Online]. Available: <https://doi.org/10.1145/3297858.3304007>
- [38] S. Tannu, Swamit and K. Qureshi, Moinuddin, "Mitigating measurement errors in quantum computers by exploiting state-dependent bias," in *Proceedings of the 52nd Annual IEEE/ACM International Symposium on Microarchitecture*, 2019, pp. 279–290.
- [39] L. Liu and X. Dou, "Qucloud: A new qubit mapping mechanism for multi-programming quantum computing in cloud environment," in *2021 IEEE International Symposium on High-Performance Computer Architecture (HPCA)*. IEEE, 2021, pp. 167–178.
- [40] P. Das *et al.*, "A case for multi-programming quantum computers," in *Proceedings of the 52nd Annual IEEE/ACM International Symposium on Microarchitecture*, 2019, pp. 291–303.
- [41] S. S. Tannu and M. Qureshi, "Ensemble of diverse mappings: Improving reliability of quantum computers by orchestrating dissimilar mistakes," in *Proceedings of the 52nd Annual IEEE/ACM International Symposium on Microarchitecture*, ser. MICRO '52. New York, NY, USA: Association for Computing Machinery, 2019, p. 253–265. [Online]. Available: <https://doi.org/10.1145/3352460.3358257>
- [42] H. Kukkonen *et al.*, "Michelson contrast, rms contrast and energy of various spatial stimuli at threshold," *Vision research*, vol. 33, no. 10, pp. 1431–1436, 1993.
- [43] D. Oliveira, E. Auden, and P. Rech, "Atmospheric neutron-induced fault generation and propagation in quantum bits and quantum circuits," *IEEE Transactions on Nuclear Science*, vol. 70, no. 4, pp. 345–353, 2023.
- [44] C. J. Wood, "Special session: Noise characterization and error mitigation in near-term quantum computers," in *2020 IEEE 38th International Conference on Computer Design (ICCD)*, 2020, pp. 13–16.
- [45] S. K. S. Hari *et al.*, "SASSIFI: An architecture-level fault injection tool for GPU application resilience evaluation," in *2017 IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS)*, 2017, pp. 249–258.
- [46] D. Deutsch and R. Jozsa, "Rapid solution of problems by quantum computation," *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences*, vol. 439, no. 1907, pp. 553–558, 1992.
- [47] E. Bernstein and U. Vazirani, "Quantum complexity theory," *SIAM Journal on computing*, vol. 26, no. 5, pp. 1411–1473, 1997.
- [48] C. H. Bennett *et al.*, "Strengths and weaknesses of quantum computing," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1510–1523, 1997. [Online]. Available: <https://doi.org/10.1137/S0097539796300933>
- [49] F. F. d. Santos *et al.*, "Analyzing and increasing the reliability of convolutional neural networks on GPUs," *IEEE Transactions on Reliability*, vol. 68, no. 2, pp. 663–677, 2019.
- [50] R. Ayanzadeh *et al.*, "Equal: Improving the fidelity of quantum annealers by injecting controlled perturbations," *arXiv preprint arXiv:2108.10964*, 2021.
- [51] J. Neumann, A. W. Burks *et al.*, *Theory of self-reproducing automata*. University of Illinois press Urbana, 1966, vol. 1102024.
- [52] D. Aharonov and M. Ben-Or, "Fault-tolerant quantum computation with constant error rate," *SIAM J. Comput.*, vol. 38, no. 4, p. 1207–1282, Jul. 2008. [Online]. Available: <https://doi.org/10.1137/S0097539799359385>
- [53] O. Fawzi, A. Grospellier, and A. Leverrier, "Constant overhead quantum fault tolerance with quantum expander codes," *Commun. ACM*, vol. 64, no. 1, p. 106–114, Dec. 2020. [Online]. Available: <https://doi.org/10.1145/3434163>
- [54] G. Li, Y. Ding, and Y. Xie, "Tackling the qubit mapping problem for nisq-era quantum devices," in *Proceedings of the Twenty-Fourth International Conference on Architectural Support for Programming Languages and Operating Systems*, 2019, pp. 1001–1014.
- [55] P. Murali *et al.*, "Software mitigation of crosstalk on noisy intermediate-scale quantum computers," in *Proceedings of the Twenty-Fifth International Conference on Architectural Support for Programming Languages and Operating Systems*, 2020, pp. 1001–1016.



Daniel Oliveira received his M.S. and Ph.D. degrees from Federal University of Rio Grande do Sul (UFRGS), Porto Alegre, Brazil, in 2013 and 2018, respectively. He is currently an assistant professor at Federal University of Paraná (UFPR) in Brazil. His current research interests include fault tolerance for HPC systems and quantum computing.

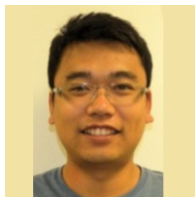


Edoardo Giusto obtained the M.S. degree in 2017 and Ph.D. degree in 2021 from Politecnico di Torino. He is currently a Research Assistant at the Department of Control and Computer Engineering at Politecnico di Torino. His research interests include WSNs, IoT, Smart Societies and Quantum Computing.



Betis Baheri Betis Baheri received his B.S. degree in Computer Science from Kent State University, in 2018, and the M.S in computer science from Kent State University in 2020. His area of research while he was in Undergraduate was security and privacy. For his master he focused on HPC systems. Previously he was working on HPC scheduler and currently he is pursuing Ph.D. degree in Computer Science at same university in quantum computing and HPC systems. His main research focus is quantum error correc-

tion, quantum deep learning, and quantum machine learning on NISQ and Ion based quantum computers.



Qiang Guan Dr. Qiang Guan is an assistant professor in Department of Computer Science at Kent State University, Kent, Ohio. Dr. Guan is the director of Green Ubiquitous Autonomous Networking System lab (GUANS). He is also a member of Brain Health Research Institute (BHRI) at Kent State University. He was a computer scientist in Data Science at Scale team at Los Alamos National Laboratory before joining KSU. His current research interests include fault tolerance design for HPC applications; HPC-

Cloud hybrid system; virtual reality; quantum computing systems and applications.



Bartolomeo Montrucchio received the M.S. degree in electronic engineering and the Ph.D. degree in computer engineering from the Politecnico di Torino, Turin, Italy, in 1998, and 2002, respectively. He is currently an Associate Professor of Computer Engineering with the Department of Control and Computer Engineering, Politecnico di Torino. His current research interests include image analysis and synthesis techniques, scientific visualization, sensor networks, RFIDs and quantum computing.



Paolo Rech received his master and Ph.D. degrees from Padova University, Padova, Italy, in 2006 and 2009, respectively. Since 2022 Paolo is an assistant professor at Università di Trento, Italy, and since 2012 he is an associate professor at UFRGS, Brazil. He is the 2019 Rosen Scholar Fellow at the Los Alamos National Laboratory, he received the 2020 impact in society award from the Rutherford Appleton Laboratory, UK and the Marie Curie Fellowship at Politecnico di Torino. His main research interests include the

evaluation and mitigation of radiation-induced effects in large-scale HPC centers and in autonomous vehicles for automotive applications and space explorations, the dependability of AI, and quantum computing.