Quantum Random Number Generators : Benchmarking and Challenges

David Cirauqui,[1,2] Miguel Ángel García-March,[2,3] Guillem Guigó Corominas,[2] Tobias Graß,[2] Przemysław R. Grzybowski,[4] Gorka Muñoz-Gil,[2,5] J. R. M. Saavedra,[1] and Maciej Lewenstein[2,6]

[1] *Quside Technologies SL, Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain*
[2] *ICFO - Institut de Ciencies Fotòniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels (Barcelona), Spain*
[3] *Instituto Universitario de Matemática Pura y Aplicada, Universitat Politècnica de València, 46022 València, Spain*
[4] *Institute of Spintronics and Quantum Information, Faculty of Physics, Adam Mickiewicz University in Poznań, Umultowska 85, 61-614 Poznań, Poland*
[5] *Institute for Theoretical Physics, University of Innsbruck, Technikerstr. 21a, A-6020 Innsbruck, Austria*
[6] *ICREA, Pg. Lluís Companys 23, 08010 Barcelona, Spain*

(Dated: June 14, 2022)

We discuss the current state of the art of Quantum Random Number Generators (QRNG) and their possible applications in the search for quantum advantages. To this aim, we first discuss a possible way of benchmarking QRNG by applying them to the computation of complicated and hard to realize classical simulations, such as critical dynamics in two-dimensional Ising lattices. These are performed with the help of computing devices based on field-programmable gate arrays (FPGAs) or graphic processing units (GPUs). The results obtained for QRNG are compared with those obtained by classical pseudo-random number generators (PRNG) of various qualities. Monte Carlo simulations of critical dynamics in moderate lattice sizes (128×128) start to be sensitive to the correlations present in pseudo-random numbers sequences, allowing us to detect them. By comparing our analysis with that of Ref. [PRE **93**, 022113 (2016)], we estimate the requirements for QRNGs in terms of speed, rapidity of access, and efficiency to achieve the objective of quantum advantage with respect to the best PRNGs. We discuss the technical challenges associated with this objective.

We dedicate this work to the memory of Roy J. Glauber and Fritz Haake, once the Masters of Kinetic Ising Models

I. INTRODUCTION

Quantum Technologies. The second and the third decade of the XXI century have witnessed the rapid developments of Quantum Technologies. In most countries, these developments are organized in four so-called "vertical pillars": quantum computation, quantum simulation, quantum metrology/sensing, and quantum communications [1]. There is also a horizontal bar connecting the four pillars, focused on basic science for Quantum Technologies, quantum software, fundamentals of quantum information science, or quantum effects in thermodynamic processes.

The universal fault-tolerant quantum computing with sufficient number of qubits and error corrections remains a dream and a severe fundamental and technological challenge. Nevertheless, the spectacular progress in noisy intermediate-scale quantum (NISQ) technologies allowed us to approach or even reach the quantum advantage (frequently termed quantum supremacy). Recently, the famous experiment by Google demonstrated efficient sampling from a random quantum circuit of 53 qubits [2]. Similar results were achieved in photon sampling [3]. Quantum simulators have achieved quantum advantage already some time ago, mainly in studying problems that belong to the area of physics (cf. [4–6]), such as static and dynamical properties of quantum many-body systems (cf. [7]). The outstanding successes of quantum metrology and sensing range from the use of squeezed states in gravitational wave detection [8] to unprecedented precision in magnetometry (for a review, see [9]). Quantum communications reached perhaps the highest technology level, as quantum cryptographic systems are widely used outside of academia and are commercially available [10, 11].

Quantum Random Number Generators. Since some applications of random numbers have to do with the security of information processing, Quantum Random Number Generators (QRNG), as a novel technology, belong to the pillar of quantum communication. Also, most of the available QRNG in academia or on the market use experimental methods and technological tools similar to quantum cryptography. The reasons for this significant interest and demand in QRNGs are manifold, including:

- All of the **classical RNGs are pseudo-random**. Typically, there is a trade-off between the statistical correlations between pseudo-random numbers *vs* their generation rate and efficiency. RNGs using iterative non-linear maps may be very fast but have typically relatively short correlation lengths. RNGs based on measuring physical or natural processes are correlated on much larger scales but are slower and less efficient. Nonetheless, combining iterative RNG with FPGA or GPU technologies, as for instance discussed in [12], might circumvent

these problems.

- If quantum mechanics is correct (which we so far believe based on striking experimental evidence), then its predictions are *intrinsically random*. In particular, this randomness can be certified in a Bell test (which, however, itself requires the use of random numbers) [13]. The philosophical, physical, and technological consequences of the randomness of quantum mechanics are discussed in great detail and from various points of view in the recent review by some of us [14]. QRNGs thus distinguish themselves from a fundamental perspective as a **remedy against pseudo-randomness**.

- Recent technical progress allows for the construction of **faster and more efficient QRNGs**, thus allowing, for instance, the first loophole-free observations of the violation of Bell inequalities and the test of non-locality of quantum mechanics [15–17].

- As such, QRNGs promise numerous **applications** in quantum cryptography in particular, as well as on areas going far **beyond quantum communications**.

Indeed, within all the different areas in which Quantum Technologies could be innovative, Random Number Generation appears as one of the fields that may benefit most from applying these new technologies.

We repeat: contrary to traditional entropy sources (e.g., thermal sources), in which we generate entropy by exploiting our lack of knowledge of the internal state of the system, quantum entropy sources are random by principle. That means that, even if we knew the whole state of the system, the outcome of the measurements remains unpredictable due to the inherently probabilistic nature of Quantum Mechanics. Moreover, this probabilistic character is fundamental; out of principle, this randomness has no internal structure, making these entropy sources fundamental for deploying the ultimate random number generators.

These ultimate randomness sources are critically important, for example, when employing randomized algorithms: procedures for efficient solving specific problems that employ random decisions in some parts of the process. Since these procedures rely on randomness, employing low-quality entropy sources can severely degrade the algorithm's efficiency and its outcome.

Plan of the paper. This paper is organized as follows. In Section II, we shortly review the technological aspects of quantum randomness following the lines of [14]. Section III explains how to benchmark RNGs using hard-to-compute, complex Monte Carlo simulations. To this aim, we devote various subsections to discuss the kinetic Ising models and the problem of calculating the dynamical critical exponent z. Last, we review the results of the Ref. [12], which stimulated our studies. Section IV contains the application of the latter methodology to PRNGs, whereas Section V presents the same methodology applied to a QRNG. Finally, Section VI presents a brief review of the literature regarding the calculation of the critical exponent; finally, we conclude in Section VII, presenting general requirements for the speed and efficiency of QRNGs to reach the quantum advantage.

II. QUANTUM RANDOMNESS AND TECHNOLOGY

Usually, when talking about the importance of random numbers, one talks about gambling and evokes the famous words of Julius Caesar: *"Alea iacta est"*. Still, *"the importance of random numbers in politics, social science and medicine should also not be underestimated; randomized polling and randomized trials are essential methodologies in these areas"* [14]. One could even add here arts: randomness plays an important role in contemporary music [18–23] and visual arts [24].

A significant challenge for randomness technologies consists of assuring non-predictability of RNG outputs - this is usually done with statistical tests [25–27], which, however, have serious drawbacks. One can summarize these drawbacks in the famous cartoon joke of Calvin [1]; or in the more profound saying of John von Neumann, *there is no such thing as a random number – there are only methods to produce random numbers* (von Neumann, 1951).

In view of these profound problems, and *"in light of the difficulties in determining the predictability of the apparent randomness seen in thermal fluctuations and other classical phenomena, using the intrinsic randomness of quantum processes is very attractive"* [14].

Recently, several methods have been proposed as QRNG candidates:

- Using device-independent (DIQIP) randomness protocols employing Bell-inequality violation, using for instance ions [28], photons [16, 17], nitrogen-vacancy centres [15], neutral atoms [29] and superconducting qubits [30]. These lead to the so-called "certified randomness" [31].

- Nevertheless, DIQIP approaches are not very efficient and fast. For practical reasons, one can use signals from quantum processes, and devices to harness the intrinsic randomness of quantum mechanics – these have existed since the 1950s. These involve devices to observe the timing of nuclear decay, [32] electron shot noise in semiconductors, splitting of photons on beamsplitters, timing of photon arrivals, vacuum fluctuations, laser phase diffusion,

[1] In the cartoon, somebody presents Calvin as a new RNG. Calvin says *Nine, nine, nine, nine, nine...* The question is: is it truly random? You never know with randomness.

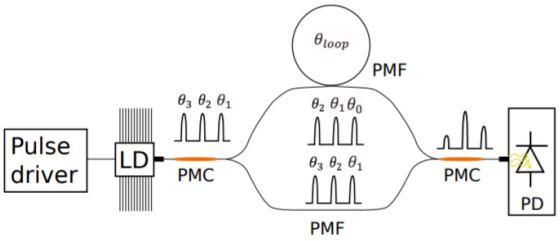

FIG. 1. **Scheme of Quside's PD-QRNG used in this work.** A laser is modulated above and below threshold, each time generating a pulse with a random phase θ_i. By means of an unbalanced Mach-Zehnder interferometer, each pulse is interfered with a later generated random phase pulse, turning phase fluctuations into intensity fluctuations, which are further converted into random numbers by using conventional photodetectors and electronics. Image taken with permission from [34].

amplified spontaneous emission, Raman scattering, atomic spin diffusion, and others. For a review on the topic, see Ref. [33].

- As for today, the fastest quantum random number generators are based on laser phase diffusion [34–37], with the record at the time of writing being 68 Gbps [38]. These devices, illustrated in Fig. 1, *"work entirely with macroscopic optical signals (the output of lasers), which greatly enhances their speed and signal-to-noise ratios. It is perhaps surprising that intrinsic randomness can be observed in the macroscopic regime, but in fact, laser phase diffusion (and before it maser phase diffusion) was one of the first predicted quantum-optical signals, described by Schawlow and Townes in 1958 (Schawlow and Townes, 1958)"*. [14].

A possible way to characterize the RNG device is via the conditional min-entropy [39],

$$H_\infty(X_i|h_i) \geq k, \quad \forall i \in \mathbb{N},\ \forall h_i, \tag{1}$$

which gives a lower bound to the unpredictability of a set of outcomes X_i from the RNG devices , given the device's history h_i, at that moment (which includes all fluctuating quantities not ascribable to intrinsic randomness). If the conditional min-entropy is bounded from below, randomness extraction techniques can be used to produce arbitrarily-high-quality output bits from the considered source.

In fact, determining the min-entropy due to intrinsic randomness of laser phase-diffusion QRNGs was a very challenging task [39], especially in the context of Bell tests [40]. Thanks to these efforts and the modeling and measurement considerations, it was possible to bound the min-entropy of these devices. In effect, laser phase diffusion random number generators have been used successfully in all loophole-free Bell tests [15–17].

III. METHODOLOGY

In this work, we propose to benchmark RNGs or QRNG by using large sequences of random numbers to perform challenging calculations, such as the Monte Carlo simulation of a complex system, whose result may be largely affected by the quality of these numbers. One should then: i) calculate a physical quantity particularly sensitive to the statistical properties of random numbers used; ii) check the results with respect to convergence and self-consistency; iii) compare the results for different RNGs, determining in this way "the best ones". This approach has been recently successfully used by Lin and Wang [12], who applied it to the calculations of the dynamical critical exponent z for a two dimensional kinetic Ising model. Below we describe with necessary details kinetic Ising models, dynamical scaling, Monte Carlo implementations and, finally, the results of Ref. [12].

Physical problem: kinetic Ising model. Randomized algorithms, such as Monte Carlo codes, are applied nowadays to a plethora of problems, ranging from the practical problems of relevance for industry and society to the purely academic ones. Among the latter, the calculation of the critical exponents associated with the phase transition of a 2D Ising model is noteworthy. In this system, there is a set of N Ising spins $\sigma_i = \pm 1$ arranged on a two-dimensional square lattice of linear side L, such that $N = L^2$. Spins are coupled by means of the coupling coefficient J_{ij}. We consider only coupling to nearest neighbors and $J_{ij} = J$ constant for all pairs of spins. The Hamiltonian that describes the statics and thermodynamics of this system is therefore

$$H = -\sum_{i,j} J_{ij}\sigma_i\sigma_j = -J\sum_{\langle i,j\rangle} \sigma_i\sigma_j, \tag{2}$$

where the sum of the term on the right is restricted to the nearest neighbours, and $1 \leq i,j \leq L$. This model is commonly used to study the behavior of ferromagnetic materials; for this purpose, periodic boundary conditions are typically used, simulating a square unit cell of size L within the periodic system under study.

The model describes the transition between the two phases of a simple ferromagnetic material: at low temperatures, most of the spins are aligned in the same direction, resulting in non-zero magnetization and ferromagnetic behavior of the material at macroscopic scales; on the contrary, at high temperatures, the fluctuations of the spins associated to thermal effects exceed the ferromagnetic order induced by the Hamiltonian; in this scenario, the spins act independently, generating zero average magnetization and thus making the material paramagnetic. The phase transition occurs when the system reaches the so-called critical temperature T_c; at this temperature, the domains of high magnetization in one direction are gradually destroyed by the effect of thermodynamic fluctuations, and converted into zones of high magnetization in

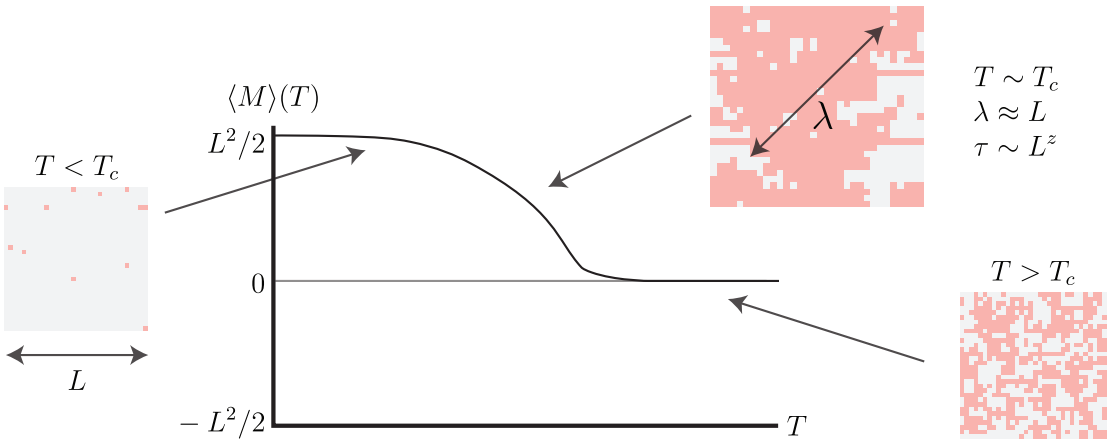

FIG. 2. **2D Ising model dynamics.** For temperatures below the critical temperature, T_c, the system shows ferromagnetic behavior; for temperatures larger than T_c, the system shows ferromagnetic behavior. At T_c, the system shows a phase transition (see main text for details).

the opposite direction. Then, macroscopically, the system is magnetized, but the orientation of the magnetic field changes in time. The time-delayed correlation of the order parameter (magnetization) is

$$\chi(t) = \langle M(t)M(0)\rangle = \sum_k a_k e^{-t/\tau_k}, \tag{3}$$

where the sum over k runs over the system's excited modes [41], M is the system's magnetization, $\tau_k = 1/\lambda_k$ is the relaxation time for the k-th excited mode, which has eigenvalue λ_k, and a_k are t-independent constants [2].

If the system is truly infinite, at the temperature approaching the critical temperature T_c, the relaxation times τ_k diverge leading to the "critical slowing down" effect. The dynamic critical scaling hypothesis [42–47] predicts that the diverging τ_k have a power-law dependence on the diverging static correlation length ξ which scales as $\xi \propto |T - T_c|^{-\nu}$. We define then the dynamic exponent z as

$$\tau_k \propto \xi^z. \tag{4}$$

Since all τ_k diverge, the relaxation process is dominated by the first excited mode with τ_1. This one effectively determines the relaxation time of the system $\tau = \tau_1$ of the whole system, so that

$$\chi(t) = \langle M(t)M(0)\rangle \propto e^{-t/\tau}. \tag{5}$$

[2] The probability of finding the system at configuration σ at time t for some initial configuration being σ_0 can be solved to be $P(\sigma, t|\sigma_0) = \sum_{k=0}^{\infty} c_k(\sigma_0) e^{-\lambda_k t}\phi_k(\sigma)$ with $\phi_k(\sigma)$ being the eigenmode with eigenvalue λ_k with standard methods (see [41] for one dimension and via Master equation, and more general methods in [42, 43])

In practice, we deal with finite systems of size $L^2 \propto M^2 = N$. This means that at T_c, the static correlation ξ grows achieving the longest wavelength $\lambda_{\max} \simeq L$. The relaxation time of the system is then expected to have a power-law relation with the $\lambda_{\max}$, i.e. for finite size scaling (FSS)

$$\tau_{\rm FSS}(L) \propto L^z. \tag{6}$$

Combining the above equations, one can determine the relaxation times and the exponent z of finite Ising lattices from Monte Carlo simulations of kinetic models, as first suggested by Hohenberg [45].

Benchmarking of randomness. The Kinetic Ising model [41] presented above belongs to a universality class called model A, or Ginzburg-Landau stochastic models without energy conservation, which are the simplest models showing slowing down critical dynamics with no conservation laws. As previously shown, this slowing down is characterized by the critical exponent z [45]. Its relaxation dynamics can be described in various ways: i) by a master equation for the time evolution of the probability distribution for one of the possible configurations of the system of spins at time t; ii) by Markovian stochastic dynamics fulfilling Fluctuation-dissipation t [41]; iii) by a Fokker-Plank equation [42, 43]. In this sense, a large body of research has pursued finding approximations for z via a variety of field theory approaches [48–65]. To the best of our knowledge, the most recent outcome from this approach is 2.14(2) for the model in two dimensions [64]. The determination of z can also be achieved via Monte Carlo (MC) simulation of the dynamics of a suitable kinetic two-dimensional Ising model, as discussed above. Many works have pursued, for more than forty years, the accurate estimation of z [66–86]. Due to the difficulty of these problem, relying on huge numbers of *random*,

MC steps, the estimation of z is highly sensitive to the quality of the random numbers employed for the simulation. The presence of correlations in random numbers may combine with the correlations generated by the kinetic Ising dynamics and the Hamiltonian themselves, resulting in mean values and variances of the critical exponent that deviate from the real value. The latter will then heavily depend on the quality of the RNG. These effects can be benchmarked by comparing the resulting z with those that would arise using a perfect randomness source.

Metropolis algorithm. Kinetic Ising Models have been studied for decades. Yet, there is no known analytical solution for two and higher dimensions: in these cases, one has to rely on approximate or numeric methods. In our study, we make use of the Metropolis algorithm [87], due to its simplicity and ease of generating an efficient implementation on hardware accelerators, such as field-programmable gate arrays (FPGAs) and Graphical processing units (GPUs). For the Metropolis algorithm, a given spin flips whenever its contribution to the total energy is reduced. However, it is also possible that the spin flips against energy minimization, subject to a certain probability that depends on the temperature. Schematically, the algorithm consists in:

- Propose a spin flip $\sigma_i \to -\sigma_i$ and compute the energy difference ΔE. If $\Delta E \leq 0$, accept the update.
- Otherwise, toss a random number $0 \leq r \leq 1$ and accept the update if $r \leq \exp(-\beta \Delta E)$.

Note that it requires an extensive use of random numbers, on the order of N^2 for one MC step per spin (this is, applying the previous recipe for all spins in the system). As we approach the critical point, the number of MC steps necessary to reach equilibrium goes to infinity due to the critical slowing down effect discussed above.

In order to parallelize computations, we split an L by L spin-lattice (with L a power of two, for the sake of simplicity of the implementation) in two different colored sublattices, in a chessboard-like fashion. This way, for a given spin, all its nearest neighbors are of its opposite color (i.e., they lie in a different sublattice) [88]. This fact prevents equally-colored spins from interacting directly and therefore allows us to update all the elements of the same sublattice in parallel. Thus, each Monte Carlo sweep is realized in two steps, each of them updating one of the sublattices in parallel; following the chessboard analogy, updating first the black squares, then the white ones.

FPGA implementation The Metropolis algorithm can be implemented directly on hardware acceleration platforms, such as field-programmable gate arrays (FPGAs). Several works have exploited FPGAs or, similarly, Graphical processing units (GPUs) to simulate spin systems (see. e.g. [12, 89–94]). By these means, we are able to directly integrate both the Ising model simulator and the quantum random number generator hardware on the same computing device, thus removing any performance bottleneck associated with data communication.

	Modulus	Multiplier	Increment
PRNG0	$2^{32}-1$	16807	0
PRNG1	$2^{25}-39$	12836191	0
PRNG2	$2^{23}-15$	422527	0
PRNG3	$2^{17}-1$	43165	0

TABLE I. Parameters used in the Linear Congruential Generators used.

This generator, designed by the company Quside Technologies, uses the phase diffusion phenomenon associated with a laser source as its source of quantum randomness (see Fig. 1). In broad terms, when the laser system is off, due to the uncertainty principle, the phase is undetermined. When the laser switches on, one of the phases is selected at random, thus defining the global phase of the laser pulse. Through laser modulation, this cycle repeats over and over again, generating a new phase that is purely random and decorrelated to the phase of the previously generated pulse.

In order to recover the phase of each pulse (which is the quantum random variable), the pulses are made to interfere with their immediate preceding ones in an unbalanced Mach-Zehnder interferometer (uMZI). The combination of amplitudes hence allows converting phase fluctuations into intensity fluctuations, which can be easily detected by a conventional photodetector. These intensity fluctuations are subsequently digitized and converted into a stream of random numbers, which feeds the Ising model simulator, thus increasing the efficiency of the system.

IV. RESULTS AND DISCUSSION

For the calculation of the critical coefficient, we simulate the spin model of Eq. 2 for a time of 1300τ and calculate its magnetization after each MC step. After inspection of Eqs. (4) and (6), we approximate τ here by $L^{z_{\text{approx}}}$ with $z_{\text{approx}} = 2$. Note that ξ, the expected theoretical value of the correlation length, equals L, since $\tau \propto \xi^z$ and $\tau_{\text{FSS}}(L) \propto L^z$. From these results, the different values of the correlation time $\tau_{\text{FSS}}(L)$ have been obtained by adjusting the correlation to a decreasing exponential for a time interval $t \in (0.3\tau_{\text{FSS}}, 1.1\tau_{\text{FSS}})$, in order to avoid both the initial high non-linearities and the fluctuations in the tail of the exponential, following Ref. [12].

A. Detecting correlation effects in PRNGs

As stated above, the dynamic exponent z is known to be sensitive to the correlations of the random numbers employed in its computation. Therefore, in order to study the effects that such correlations have in our results, we make use of different PRNGs to simulate our system.

a. Fundamental tests with different PRNGs Before introducing the calculation with the QRNGs, we address the computation of the dynamic exponent with four different linear congruential generators (LCGs)-based generators, all of them presumably showing low correlations [95]. Generally, an LCG of the form $x_{i+1} = (ax_i + c) \bmod m$ is described by three different parameters: its modulus m, its multiplier a, and increment c. The modulus sets its period of repetition; once selected, the other two parameters may be tuned such that the generator exhibits low correlations.

Regarding the simulation procedure, there are a couple of questions worth commenting. The first one regards an estimation of the total amount of random numbers required per lattice sweep, which in our case will be $n_{\text{par}} = L^2$, for a lattice with L sites per side (see Appendix A for a detailed discussion on the the quantity of random numbers required by our codes, and possible routes for future optimization). Second, given the suitability of GPU architectures for solving Ising-like problems, we implement our PRNGs and kinetic Ising algorithms in such a device in order to test the performance of the different PRNGs. We can also take advantage of its single-instruction multiple-thread (SIMT) execution model in order to avoid the pseudo-random number generation bottleneck. To do so, we implement a GPU kernel that, given the L^2 seeds, produces L^2 new PRNs in parallel, employing highly tested and consolidated LCGs that exhibit low correlations [95]. Using LCGs also allows us to tune their parameters easily, and therefore explore the effect that the correlations appearing in PRN sequences have on the results of our MC simulations.

With each PRNG and for each lattice size (ranging from $L = 4$ to $L = 512$), we compute the dynamic exponent z with a Monte Carlo simulation. In Table I we give the parameters used for each generator [95]. For each point in the simulation, we run a total number of $N_{it} \geq 100$ iterations in order to extract statistically relevant results (the number of iterations is restricted to $N_{it} \sim 10$ for $L = 512$ lattices, due to long computation times). We fit the obtained curves with exponential laws in order to obtain τ for different lattice sizes, and then plot them in a logarithmic scale as a function of the lattice size to obtain the dynamic exponent z. We then compare them with the theoretical estimate of z obtained by studying the stochastic matrices governing the physics of our system in the classical Ref. [85], that is, $z = 2.1667 \pm 0.0005$. We summarize our results in Table II, in which we show the obtained dynamic exponents z, as well as their respective errors relative to the theoretical estimate, ϵ_r (we take as reference $z_{\text{ref}} = 2.1667$ and approximate ϵ_r in the fourth decimal).

	z	ϵ_r
PRNG0	2.1087	0.0268
PRNG1	2.1159	0.0234
PRNG2	2.1047	0.0286
PRNG3	2.1162	0.0233

TABLE II. Dynamic exponents z and relative errors with respect to theoretical estimate ϵ_r, obtained for each PRNG.

All tested PRNG's yield a reasonable approximation of the dynamic exponent, as can be seen in Table II, but they differ in their predicted value in the second significant decimal.

Importantly, the statistical variance of the results poses a considerable caveat that must be taken into account when interpreting them. For any given PRNG, once the amount of random numbers consumed by the algorithm exceeds its period of repetition (modulus in Table I), the sequence repeats itself, introducing a large amount of correlation at large time scales. We observe that these extra correlations affect the obtained dynamic exponent by exponentially enlarging the variance between iterations of the same simulation while keeping its mean value constant. To quantify these correlations, we define the normalized variance as σ^2/μ^2, where σ is the variance of the results and μ their mean value. For this case, the normalized variance stays more or less constant (around a value of $\frac{\sigma^2}{\mu^2} \approx 0.01$), until the lattice reaches a size large enough so that its simulation requires more random numbers than the generator's period of repetition. Beyond this point, the variance starts to increase exponentially with lattice size, as shown in Fig. 3. Furthermore, as we keep increasing L far beyond the variance's explosion point, the obtained magnetization autocorrelation function $\chi(t)$ does no longer resemble an exponential decay, but instead starts showing a noisy behavior (not shown). Therefore one cannot strictly speak of, nor extract, a reliable value for the dynamic exponent.

b. Effects of reseeding. We now explore a natural question: how does the reseeding of the generators affect the results presented in previous paragraph, since the addition of physically random bits yields a theoretically infinite-period PRNG [12]? We again study the behavior of the normalized variance in our Ising system by physically reseeding the same PRNG3 used in the previous section (which itself constitutes a computationally hard task). We reseed it every $\kappa(m-1)$ pseudo-random numbers, where m is the modulus parameter of the LCG, and we first consider $\kappa = \{1, 2, 4, 8\}$. As shown in Fig. 4, we find that, for all cases, the variance explosion observed before is avoided. In this case, the normalized variance does not grow monotonically, but instead reaches a plateau whose value appears to be proportional to the number of repetitions introduced in the pseudo-random

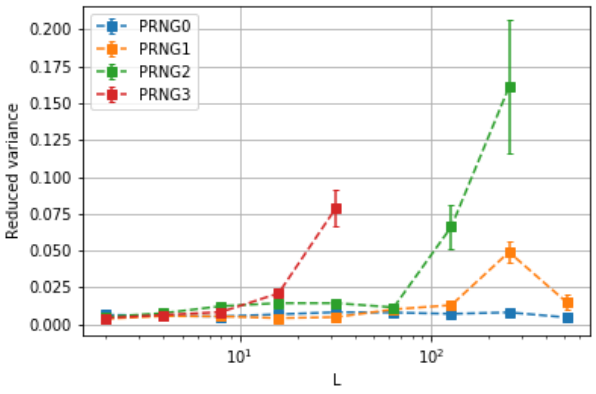

FIG. 3. Statistical variance of the dynamic exponent z, normalized to its mean value, obtained from $N_{it} \geq 100$ iterations for all points except for $L = 512$, for which $N_{it} = 30$, as a function of lattice size, for different PRNG's

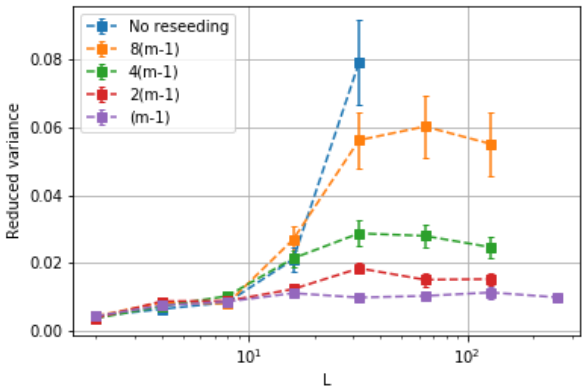

FIG. 4. Normalized variance for PRNG3 as a function of lattice size. Physical reseeding of the generator every $(m-1)$, $2\,(m-1)$, $4\,(m-1)$, $8\,(m-1)$ random numbers. PRNG3 without reseeding is shown for comparison.

sequences before the reseeding is carried out (i.e., the amount of extra correlations introduced in our algorithm, compared to the infinite-period PRNG).

As shown in Fig. 4, the case $\kappa = 1$, i.e. an example of an infinite-period pseudo-random number generator, exhibits the lowest normalized variance of all presented cases. Interestingly, by allowing $\kappa < 1$ (and thus paying the computational cost associated with a high-frequency reseeding), we observe that we can still lower this value further down (see Fig. 5). This scenario minimizes the correlations appearing in the pseudo-random sequences, approaching a true RNG (TRNG) as κ gets smaller. Therefore, this fact allows us to conclude that *the use of PRNG's, even those showing low correlations and having a theoretically infinite period, can indeed affect the quality of our results in terms of variance* for the problem at hand. Moreover, as we show here, once κ is fixed, the variance of the obtained z converges to a plateau and barely changes with L. Hence, performing longer simulations will not improve the approximation.

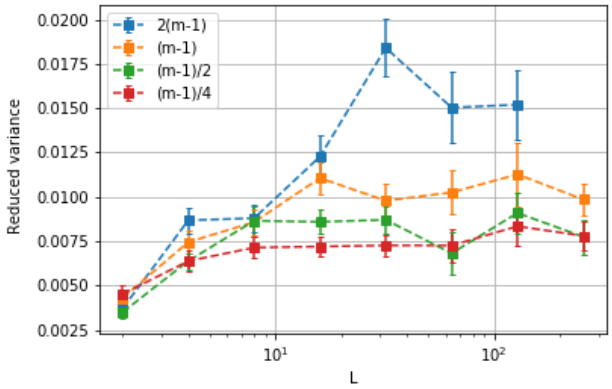

FIG. 5. Normalized variance for PRNG3 as a function of lattice size. Physical reseeding of the generator every $2\,(m-1)$, $(m-1)$, $\frac{(m-1)}{2}$ and $\frac{(m-1)}{4}$ random numbers.

Next, we extract the values of the reduced variance plateaus and plot them as a function of the reseeding period κ. Interestingly, as shown in Fig. 6, both quantities show a linear relation. By means of a linear fitting, we then can extrapolate the reduced variance for $\kappa = 0$, this is, the case of a TRNG. We obtain a value of $\frac{\sigma^2}{\mu^2}(\kappa = 0) \approx 0.004$, which coincides with the initial points of the curves of Figs. 4 and 5, corresponding to simulations of very small latices, where correlations between pseudo random numbers are still non-detectable.

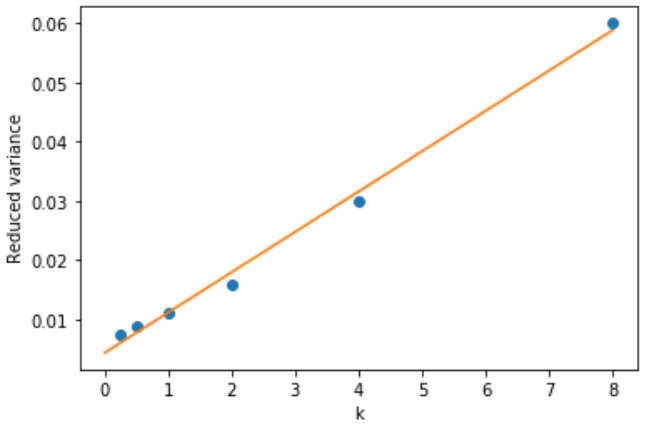

FIG. 6. Reduced variance for different values of the reseeding period κ of PRNG3 (dots) and linear fit (line).

On top of the presented effect on the variance of the estimation of the dynamic exponent z, we also analyze its mean value for different κ. We observe that the reseeding of the generators yields a more accurate result for the

mean value of the dynamic exponent (see Table III). We note that, for every case with reseeding, and for every frequency κ implemented, the relative error to the theoretical value is reduced to about half the one obtained with the different PRNG's used in Table II, which were not reseeded. Nevertheless, we cannot reduce this error further. We emphasize that reducing κ reduces the variance, bringing the result closer to those of a TRNG, but at a larger computational cost for smaller and smaller κ. The results here point out that in the limit of very small κ, one should obtain results close to those obtained with a TRNG. Nonetheless, there is no practical way of testing this due to the large computational cost.

	z	ϵ_r
$\kappa = 2$	2.1815	0.0068
$\kappa = 1$	2.1477	0.0088
$\kappa = \frac{1}{2}$	2.1482	0.0085
$\kappa = \frac{1}{4}$	2.1441	0.0104

TABLE III. Dynamic exponents z and relative errors with respect to theoretical estimate ϵ_r, for different reseeding frequencies of PRNG3.

V. CALCULATION OF THE DYNAMIC CRITICAL EXPONENT z WITH A QRNG

In this section, we present the results on the calculation of the dynamical critical exponent using a FPGA and, most importantly, a quantum RNG (QRNG). As in previous sections, we performed simulations for different lattice sizes. In Fig. 7 we show the time-delayed correlation of the order parameter (magnetization), $\chi(t)$, as a function of time. We see the expected exponential decay described by Eq. (5). By fitting the previous equation, we extract the average value of the exponent τ for each L. We performed 100 simulations for L up to 256 and 15 simulations for $L = 512$ due to the large computational cost in this last case (see discussion below). It is very apparent from last panel in Fig. 7 that the results for $L = 512$ are more noisy that those obtained for smaller lattice sizes, probably due to the smaller number of simulations.

In Fig. 8 we represent the average correlation time $\tau(L)$ obtained from these results. Performing a linear fitting of the obtained curve, we find a value of the critical exponent $z = 2.165 \pm 0.039$. We emphasize that, from here, there is a clear strategy to improve this value: performing multiple simulations for bigger lattices would add more points to the fit, resulting in a better approximation of this coefficient. However, unlike the case of pseudo-generators, obtaining correlation times for larger cell sizes is limited by the vast need for random numbers required by the simulation. Note that, for each step of the simulation, $N \propto L^2$ random numbers are required. As the simulations are run for $1300\tau_k = 1300L^z$ steps, we require on the order of $1300L^{z+2}$ random numbers. Assuming that each of these numbers has 32-bit precision, we face a massive consumption of about $41600 \cdot L^{z+2}$ randomly-distributed bits. For small cell sizes, these requirements are innocuous; however, the $\sim L^4$ exponential growth in demand for random numbers is prohibitive. In the case of Quside's QRNG apparatus used in our simulations, which reaches quantum random number generation rates of 400 Mbps, we spend around 12 hours for each simulation of $L = 256$. Doubling the size of the network (L =512) requires twenty days for each simulation; by doubling it again ($L = 1024$), we estimate a simulation time of almost six months per simulation. To avoid this computational bottleneck, and speeding-up the simulation of the $L = 512$ case, we used an amplification of the QRNG's random numbers. This amplification consists on the implementation of a PRNG on the FPGA, which is reseeded as fast as the QRNG provides new seeds. . This decision introduces some correlations that are not present for smaller lattices. This fact, along the very low number of repetitions, could potentially be the reason of the more noisy behaviour observed in the last panel of fig.7, as discussed in the PRNG section. Nevertheless, due to the small size of the statistical sample at hand, we cannot conclude which one of them is the predominant reason without additional simulations.

VI. VALUES OF THE DYNAMICAL CRITICAL EXPONENT IN THE SCIENTIFIC LITERATURE

Before concluding, we offer in this section a discussion and review of previous results. Over the years, many attempts to give an appropriate value for the dynamical critical exponent z have been carried on from theoretical, experimental and MC sides. Here, with the aim of illustrating how vastly the obtained results vary, we present a long, yet non-exhaustive collection of values found in the literature, for both two- and three- dimensional lattices. Some of the references presented here give various values corresponding to different types of lattices, in an attempt to show the postulated universality of z across models. We plot in Fig. 9 the obtained exponents as a function of the year of its calculation. Surprisingly, even with the expected improvement in the used methods, there is no clear tendency, neither in two-, three-dimension, theoretical or MC calculations, and even the various results obtained in recent years show a wide spreading. The data is gathered in Tables VI and VII from Appendix C. We plot in Fig. 9b a histogram grouping the theoretical predictions and the MC ones. While the values obtained by means of theoretical methods do not show any apparent distribution, the ones obtained with MC calculations can be fitted to a Gaussian distribution with mean $\langle z_{\mathrm{MC}} \rangle = 2.1664$. Importantly, such value is close to the one predicted by our QRNG calculations. While this is not conclusive, it clearly shows the importance of pushing forward the research conducted in this paper to larger

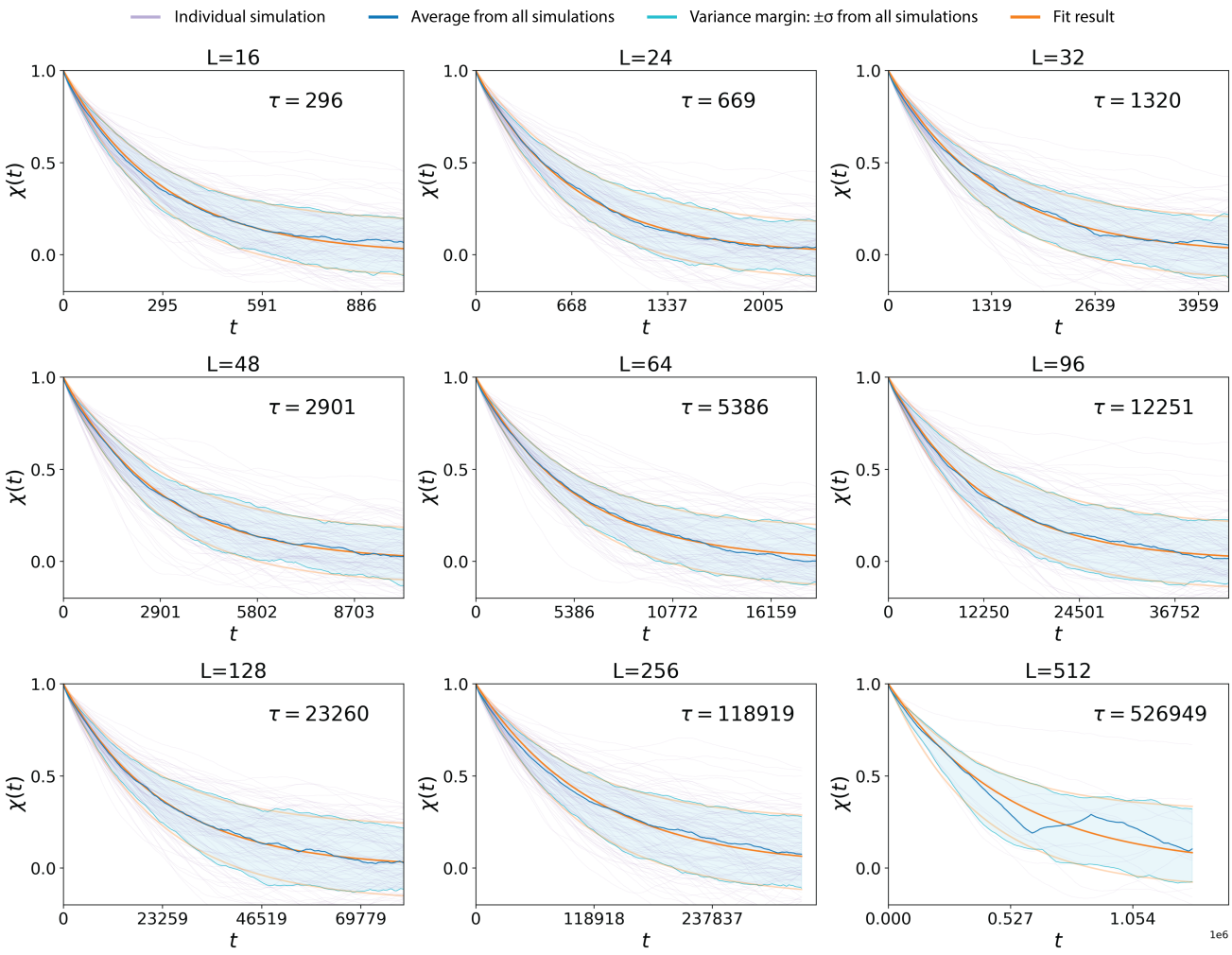

FIG. 7. **Determination of the relaxation time as a function of lattice size.** Inset τ values are the decay times associated to the orange curves, which correspond to the averages obtained by the fitting of the multiple repetitions simulated at each side length. The individual simulations (purple), as well as the variance interval for all of them (cyan) are also shown in the graphs.

lattice sizes and more repetitions, given that the QRNG do not have the variance limitation of the PRNG.

VII. CONCLUSIONS AND OUTLOOK

In this work, we have studied the effect of different random number sources in highly complex computational tasks. We have shown that the correlations appearing in pseudo-random number sequences greatly affect the results obtained when computing the dynamic critical exponent of the Ising model. First, we showcased that once the period of repetition of the PRNG is reached (and therefore significant correlations start to appear), the variance of our results explodes. Nonetheless, we have also shown that, reducing the correlations introduced by the repetition of the sequences by reseeding our generators, such variance explosion can be avoided, reaching a value that depends on the frequency at which the reseeding is carried on. In this direction, by extrapolating the values obtained for different reseeding frequencies, we have also estimated an upper bound for the variance that should be expected when using a true random number generator. The reseeding of the generators also affects the mean value of the obtained dynamic exponent, making it closer to the theoretical estimate. We can therefore state that, the closer a RNG is to a true RNG, the better the estimation of the dynamics exponent, both in terms of mean and variance.

To avoid the aforementioned problems, we have shown a new promising avenue: the use of quantum random number generator. The first explorations on the matter, presented in this work, yield a mean value of the critical exponent z in accordance with majority of results proposed in literature. While the results obtained in this work are encouraging and show the potential of QRNG for complex simulations, we believe that further improvements need to be done in order to be conclusive on this

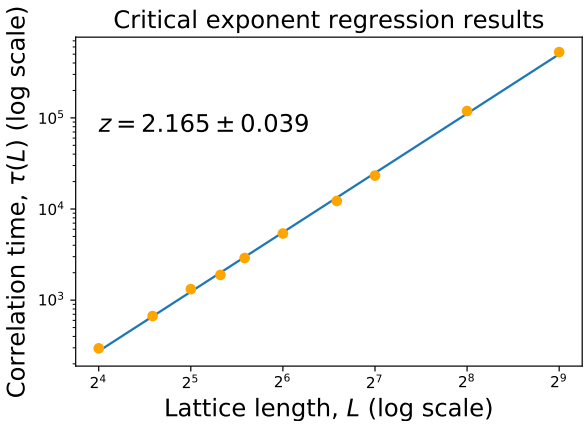

FIG. 8. *Critical exponent calculation with a Quantum Random Numbers source.* Orange: estimated relaxation times (in log10 scale) as a function of the lattice size (in log2 scale); blue, the linear fitting $\log_2(\tau) = z \cdot \log_2(L) + b$ associated. The slope of the fitting $z = 2.165 \pm 0.039$ corresponds to the critical exponent, in agreement with theoretical results.

value. For this, the random number generation speed is still the current simulation bottleneck, as shown in Appendix A, making it difficult to get enough statistics when using properly guaranteed, quantum randomness. Nonetheless, the recent advances in the field point towards such achievement. Then, if it is shown that the QRNG results converge towards a stable and conclusive critical exponent for large lattices, yielding a variance equal or lower to the bound estimated in this work, the use of the Ising model's critical exponent calculation as a benchmarking tool for other randomness generators will be greatly justified, by merely contrasting the latter with the results obtained by the QRNG.

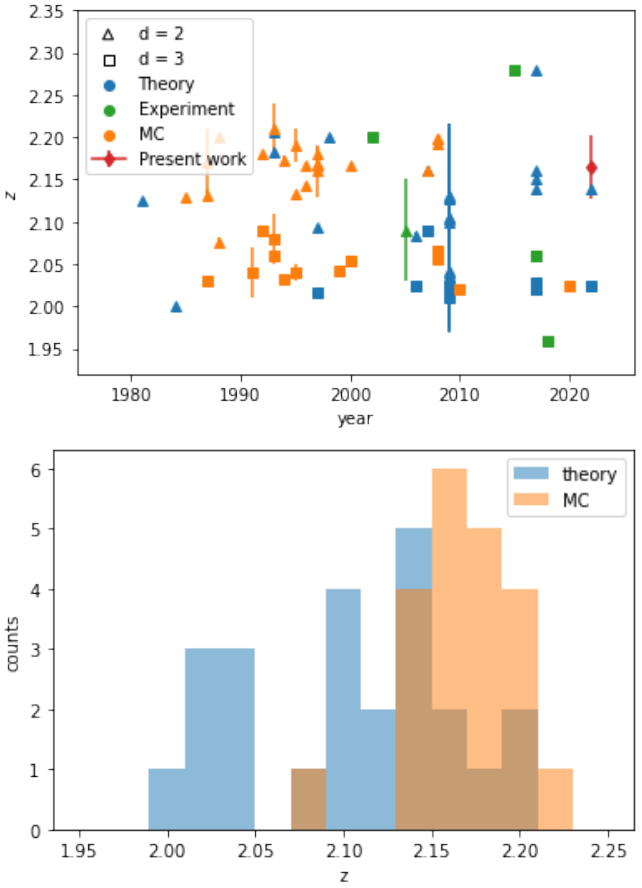

FIG. 9. *Dynamical critical exponents given in the literature.* Top: Different z calculated over the years in two and three dimensions. Triangles and squares label two- and three- dimensional lattices, while colors blue, green and orange mark whether these values were obtained theoretically, experimentally or via MC simulations, respectively. The value obtained in the present work is marked with a red diamond. Bottom: Histogram showing the z predictions theoretically and with MC in two dimensions.

ACKNOWLEDGMENTS

We acknowledge Joana Frexanet, Lluis Torner, Sergi Ferrando, Pau Gómez, Felix Tebbenjohanns, and Carlos Abellán. We acknowledge also discussions with Josep Maria Martorell, Mervi Mantsinen, Xavier Saez, Vassil Alexandrov, Francisco Castejón, and Shinsuke Satake in the early stage of this project. We acknowledge ERC AdG NOQIA; Agencia Estatal de Investigación (R&D project CEX2019-000910-S, funded by MCIN/ AEI/10.13039/501100011033, Plan Nacional FIDEUA PID2019-106901GB-I00, FPI, QUANTERA MAQS PCI2019-111828-2, Proyectos de I+D+I "Retos Colaboración" QUSPIN RTC2019-007196-7), MCIN via European Union NextGenerationEU (PRTR-C17.I1); Fundació Cellex; Fundació Mir-Puig; Generalitat de Catalunya through the European Social Fund FEDER and CERCA program (AGAUR Grant No. 2017 SGR 134, QuantumCAT / U16-011424, co-funded by ERDF Operational Program of Catalonia 2014-2020); EU Horizon 2020 FET-OPEN OPTOlogic (Grant No 899794); National Science Centre, Poland (Symfonia Grant No. 2016/20/W/ST4/00314); European Union's Horizon 2020 research and innovation programme under the Marie-Skłodowska-Curie grant agreement No 101029393 (STREDCH) and No 847648 ("La Caixa" Junior Leaders fellowships ID100010434: LCF/BQ/PI19/11690013, LCF/BQ/PI20/11760031, LCF/BQ/PR20/11770012, LCF/BQ/PR21/11840013). D.C.G. acknowledges funding from Generalitat de Catalunya (AGAUR Doctorats Industrials 2019, 2n termini). MAGM acknowledges funding from the Spanish Ministry of Education and Professional Training (MEFP) through the Beatriz Galindo program 2018 (BEAGAL18/00203). G.M-G. acknowledges support from the Austrian Science Fund (FWF) through SFB BeyondC F7102.

APPENDICES

Appendix A: Parallelization using FPGAs/GPUs: required number of random numbers

Note that our code runs over every single spin at any time step. This updating process differs from other possible implementations of the Metropolis algorithm that rely on sequential updates such as sampling and updating L^2 (with L the lattice size) spins for each iteration, with the spins selected at random. Such a sequential implementation does not guarantee that all of the spins will be given the chance of being updated, nor that all of them will be updated only once in each Monte Carlo sweep (even if it does satisfy ergodicity in the long run). This fact does not make a difference in the obtained results [93], but yields a considerable improvement in performance when using the parallel Metropolis version. Not only it allows the spins to be updated in a parallel manner, but it also reduces the entropy consumption of the algorithm since it does not require such L^2 random numbers at every time step that chooses the spins to be updated. On the other hand, our implementation assumes that every single spin might be asked to flip with a certain probability following the Metropolis algorithm, thus consuming again L^2 random numbers, while a CPU-based code would only need a fraction $\alpha \leq 1$ of them, corresponding to these spins that are not flipped directly after computing its energy difference between both initial and proposed states.

Taking everything into account, a sequential algorithm consumes $n_{\text{seq}} = L^2(1+\alpha)$ random numbers at every time step, while the parallel one only demands $n_{\text{par}} = L^2$, which equals the best lower bound achievable with a sequential device. In this direction, our code could be further optimized in order to avoid the discard of the $L^2(1-\alpha)$ numbers that are not used in the previous iteration, replacing these ones consumed, and therefore yielding a much lower demand of $n_{\text{par}} = L^2\alpha$.

L	MC updates/ simulation	N_{it}	Random bits/ update	Total bits required (GB)	Simulation time (days)
16	533192	100	512	3.2	0.001
24	1285292	100	1152	17.2	0.006
32	2399489	100	2048	57.2	0.02
48	5784114	100	4608	310.3	0.1
64	10798263	100	8192	1029.8	0.3
96	26029866	100	18432	5585.4	1.9
128	48594709	100	32768	18537.4	6.1
256	218687559	100	131072	333690.7	111
512	984145175	10	524288	600674.5	199
			TOTAL	959905.8	318

TABLE IV. Estimated randomness consumption and simulation times for the QRNG results.

When implementing the code in a GPU, we note that, given the availability of GPU resources, the possible optimization of the PRN generation introduced in previous paragraph would not yield any improvement. It is also worth noting that such optimization would introduce even more correlations in the results: by possibly discarding some random numbers, we indeed lower the correlation between the probabilities used by a given spin to be updated at two different times.

Appendix B: Linear fit of the dynamic exponent.

As discussed in previous sections, the relaxation time of the system is expected to have a power-law relation with the lattice size L. In order to obtain the dynamic exponent z, one can take logarithms to both sides of Eq. (6) by naively reducing it to an equality $\tau = L^z$ and then make a linear fit $\log(\tau) = z\log(L)$. Instead, we strictly consider the proportional sign in Eq. (6) by stating that $\tau = \tau_0 L^z$, therefore allowing the linear fit to have an offset, $\log(\tau) = z\log(L) + \log(\tau_0)$.

We summarize our findings in Section V, in which we compare the offset obtained by the fitting of the QRNG data against those obtained by the PRNG data. There are two main things worth noting about the obtained results. First, we observe that all of them yield a non-zero, negative offset. And, secondly, we note that those PRNG using reseeding (thus having an infinite period, and therefore being closer to a TRNG) yield values closer to the one obtained by the QRNG. This fact hints that this parameter could potentially serve in the purpose of discerning good from bad randomness too.

	$log(\tau_0)$
QRNG	-0.362
PRNG3 $k = \frac{1}{2}$	-0.1701
PRNG3 $k = 2$	-0.2454
PRNG2	-0.0906
PRNG0	-0.1007
PRNG1	-0.1183

TABLE V. Results obtained for $log(\tau_0)$ by using different RNG. These values correspond to the fittings yielding the dynamic exponents shown in previous sections.

Appendix C: Summary of all calculated dynamical critical exponents, for two and three dimension.

In Tables VI and VII we gather all calculated exponents from the literature in two and three dimensions, to the best of our knowledge, for theoretical, MC as well as experimental approaches. This is the data plotted in Fig. 8.

[1] A. Acín, I. Bloch, H. Buhrman, T. Calarco, C. Eichler, J. Eisert, D. Esteve, N. Gisin, S. J. Glaser, F. Jelezko, *et al.*, New Journal of Physics **20**, 080201 (2018).

[2] F. Arute, K. Arya, R. Babbush, *et al.*, Nature **574**, 505–510 (2019).

[3] H.-S. Zhong, H. Wang, Y.-H. Deng, M.-C. Chen, L.-C. Peng, Y.-H. Luo, J. Qin, D. Wu, X. Ding, Y. Hu, P. Hu, X.-Y. Yang, W.-J. Zhang, H. Li, Y. Li, X. Jiang, L. Gan, G. Yang, L. You, Z. Wang, L. Li, N.-L. Liu, C.-Y. Lu, and J.-W. Pan, Science **370**, 1460 (2020), https://www.science.org/doi/pdf/10.1126/science.abe8770.

[4] A. Trabesinger, Nature Physics **8**, 263–263 (2012).

[5] M. Lewenstein, A. Sanpera, and V. Ahufinger, *Ultracold Atoms in Optical Lattices: Simulating quantum many-body systems* (Oxford University Press, Oxford, 2012).

[6] J. Fraxanet, T. Salamon, and M. Lewenstein, Lecture Notes in Physics **1000** (2017).

[7] S. Trotzky, Y. Chen, A. Flesch, *et al.*, Nat. Phys. **8**, 325–330 (2012).

[8] J. Aasi *et al.*, Nat. Photonics **7**, 613–619 (2013).

[9] D. Braun, G. Adesso, F. Benatti, R. Floreanini, U. Marzolino, M. W. Mitchell, and S. Pirandola, Rev. Mod. Phys. **90**, 035006 (2018).

[10] S. Pirandola, U. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, and C. Ottaviani, arXiv preprint arXiv:1906.01645 (2019).

[11] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Reviews of modern physics **74**, 145 (2002).

[12] Y. Lin and F. Wang, Phys. Rev. E **93**, 022113 (2016).

[13] M. Rowe, D. Kielpinski, V. Meyer, *et al.*, Nature **409**, 791–794 (2001).

[14] M. N. Bera, A. Acín, M. Kuś, M. W. Mitchell, and M. Lewenstein, Reports on Progress in Physics **80**, 124001 (2017).

[15] B. Hensen, H. Bernien, A. Dréau, *et al.*, Nature **526**, 682–686 (2015).

[16] M. Giustina, M. A. M. Versteegh, *et al.*, Phys. Rev. Lett. **115**, 250401 (2015).

[17] L. K. Shalm, E. Meyer-Scott, *et al.*, Phys. Rev. Lett. **115**, 250402 (2015).

[18] A. Whittall, *Serialism (Cambridge Introductions to Music)* (Cambridge University Press, 2008).

[19] K. H. Wörner, *Stockhausen; Life and Work.* (Univ of California Pr, 1973).

[20] K. Boehmer, *Zur Theorie der offenen Form in der neuen Musik*, Vol. 1 (Tonos, 1967).

[21] P. Boulez, *Relevés d'apprenti* (Seuil, 1966).

[22] R. Yamada, S. Grandi, G. Muñoz-Gil, L. Barbiero, A. Aloy, and M. Lewenstein, arXiv preprint arXiv:2109.03511 (2021).

[23] R. Yamada and M. Lewenstein, Interpreting quantum randomness, AI & Music S+T+ARTS (2021), https://www.youtube.com/watch?v=Z-GLxgg0Z18.

[24] Tate museum - abstract expressionism, https://www.tate.org.uk/art/art-terms/a/abstract-expressionism; (accessed 11-January-2020).

[25] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, *A statistical test suite for random and pseudorandom number generators for cryptographic applications*, Tech. Rep. (Booz-Allen and Hamilton Inc Mclean Va, 2001).

[26] G. Marsaglia, W. W. Tsang, *et al.*, Journal of Statistical Software **7**, 1 (2002).

[27] D. Eddelbuettel and R. G. Brown, Initial Version as of May (2007).

[28] S. Pironio, A. Acín, S. Massar, *et al.*, Nature **464**, 1021–1024 (2010).

[29] W. Rosenfeld, M. Weber, J. Volz, F. Henkel, M. Krug, A. Cabello, M. Zukowski, and H. Weinfurter, Advanced science letters **2**, 469 (2009).

[30] M. Jerger, Y. Reshitnyk, M. Oppliger, *et al.*, Nat. Commun. **7**, 12930 (2016).

[31] A. Acín and L. Masanes, Nature **540**, 213–219 (2017).

[32] M. Isida and H. Ikeda, Annals of the Institute of Statistical Mathematics **8**, 119 (1956).

[33] M. Herrero-Collantes and J. C. Garcia-Escartin, Rev. Mod. Phys. **89**, 015004 (2017).

[34] C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. W. Mitchell, Opt. Express **22**, 1645 (2014).

[35] M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell, and V. Pruneri, Opt. Express **19**, 20665 (2011).

[36] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, Opt. Express **20**, 12366 (2012).

[37] Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Fröhlich, A. Plews, and A. J. Shields, Appl. Phys. Lett. **104**, 261112 (2014).

[38] Y.-Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J.-W. Pan, Review of Scientific Instruments **86**, 063105 (2015).

[39] M. W. Mitchell, C. Abellan, and W. Amaya, Phys. Rev. A **91**, 012314 (2015).

[40] C. Abellán, W. Amaya, D. Mitrani, V. Pruneri, and M. W. Mitchell, Phys. Rev. Lett. **115**, 250403 (2015).

[41] R. J. Glauber, J. Math. Phys **4**, 294 (1963).

[42] S.-K. Ma, *Modern theory of critical phenomena* (Routledge, 2018).

[43] J. Zinn-Justin, *Quantum field theory and critical phenomena* (Clarendon Press, 1996).

[44] B. Halperin and P. Hohenberg, Physical Review **177**, 952 (1969).

[45] P. C. Hohenberg and B. I. Halperin, Rev. Mod. Phys. **49**, 435 (1977).

[46] M. Suzuki, Progress of Theoretical Physics **58**, 1142 (1977).

[47] G. Ódor, Reviews of modern physics **76**, 663 (2004).

[48] B. I. Halperin, P. C. Hohenberg, and S.-k. Ma, Phys. Rev. Lett. **29**, 1548 (1972).

[49] C. De Dominicis, E. Brézin, and J. Zinn-Justin, Phys. Rev. B **12**, 4945 (1975).

[50] Z. Rácz and M. F. Collins, Phys. Rev. B **13**, 3074 (1976).

[51] R. Bausch, V. Dohm, H. K. Janssen, and R. K. P. Zia, Phys. Rev. Lett. **47**, 1837 (1981).

[52] E. Domany, Phys. Rev. Lett. **52**, 871 (1984).

[53] B. Dammann and J. D. Reger, Europhysics Letters (EPL) **21**, 157 (1993).

[54] J. Wang, Phys. Rev. B **47**, 869 (1993).

[55] V. Prudnikov, S. Belim, E. Osintsev, and A. Fedorenko, Physics of the Solid State **40**, 1383 (1998).

[56] J.-S. Wang and C. K. Gan, Phys. Rev. E **57**, 6548 (1998).

[57] R. Folk and G. Moser, Journal of Physics A: Mathematical and General **39**, R207 (2006).

[58] A. Krinitsyn, V. V. Prudnikov, and P. V. Prudnikov, Theoretical and mathematical physics **147**, 561 (2006).

[59] L. Canet and H. Chaté, Journal of Physics A: Mathematical and Theoretical **40**, 1937 (2007).

[60] M. Y. Nalimov, V. Sergeev, and L. Sladkoff, Theoretical and Mathematical Physics **159**, 499 (2009).

[61] E. Lubetzky and A. Sly, Communications in Mathematical Physics **313**, 815 (2012).

[62] D. Mesterházy, J. H. Stockemer, and Y. Tanizaki, Phys. Rev. D **92**, 076001 (2015).

[63] C. Duclut and B. Delamotte, Phys. Rev. E **95**, 012107 (2017).

[64] L. Adzhemyan, D. Evdokimov, M. Hnatič, E. Ivanova, M. Kompaniets, A. Kudlis, and D. Zakharov, Physics Letters A **425**, 127870 (2022).

[65] N. O. Silvano and D. G. Barci, arXiv preprint arXiv:2112.01547 (2021).

[66] H. C. Bolton and C. H. J. Johnson, Phys. Rev. B **13**, 3025 (1976).

[67] J. K. Williams, Journal of Physics A: Mathematical and General **18**, 49 (1985).

[68] N. Ito, M. Taiji, and M. Suzuki, Journal of the Physical Society of Japan **56**, 4218 (1987).

[69] S. Tang and D. Landau, Physical Review B **36**, 567 (1987).

[70] N. Ito, M. Taiji, and M. Suzuki, Le Journal de Physique Colloques **49**, C8 (1988).

[71] M. Mori and Y. Tsuda, Physical Review B **37**, 5444 (1988).

[72] A. M. Ferrenberg, D. P. Landau, and K. Binder, Journal of statistical physics **63**, 867 (1991).

[73] D. Stauffer, Physica A: Statistical Mechanics and its Applications **184**, 201 (1992).

[74] N. Ito, Physica A: Statistical Mechanics and its Applications **196**, 591 (1993).

[75] C. Münkel, D. W. Heermann, J. Adler, M. Gofman, and D. Stauffer, Physica A: Statistical Mechanics and its Applications **193**, 540 (1993).

[76] P. Grassberger, Physica A: Statistical Mechanics and its Applications **214**, 547 (1995).

[77] U. Gropengiesser, Physica A: Statistical Mechanics and its Applications **215**, 308 (1995).

[78] Z. Li, L. Schülke, and B. Zheng, Physical review letters **74**, 3396 (1995).

[79] Z. Li, L. Schülke, and B. Zheng, Phys. Rev. E **53**, 2940 (1996).

[80] M. Nightingale and H. Blöte, Physical review letters **76**, 4548 (1996).

[81] M. Silvério Soares, J. Kamphorst Leal da Silva, and F. C. SáBarreto, Phys. Rev. B **55**, 1021 (1997).

[82] F.-G. Wang and C.-K. Hu, Phys. Rev. E **56**, 2310 (1997).

[83] C. Godreche and J. Luck, Journal of Physics A: Mathematical and General **33**, 9141 (2000).

[84] N. Ito, K. Hukushima, K. Ogawa, and Y. Ozeki, Journal of the Physical Society of Japan **69**, 1931 (2000), https://doi.org/10.1143/JPSJ.69.1931.

[85] M. P. Nightingale and H. W. J. Blöte, Phys. Rev. B **62**, 1089 (2000).

[86] X. Lei, J. Zheng, and X. Zhao, Chinese Science Bulletin **52**, 307 (2007).

[87] N. Metropolis, A. W. Rosenbluth, M. N. Rosenbluth, A. H. Teller, and E. Teller, The journal of chemical physics **21**, 1087 (1953).

[88] M. Weigel, Order, Disorder and Criticality **5**, 271 (2017).

[89] M. C. Herbordt, T. VanCourt, Y. Gu, B. Sukhwani, A. Conti, J. Model, and D. DiSabello, Computer **40**, 50 (2007).

[90] F. Belletti, M. Cotallo, A. Cruz, L. A. Fernandez, A. Gordillo, A. Maiorano, F. Mantovani, E. Marinari, V. Martin-Mayor, A. Munoz-Sudupe, *et al.*, Computer Physics Communications **178**, 208 (2008).

[91] T. Preis, P. Virnau, W. Paul, and J. J. Schneider, Journal of Computational Physics **228**, 4468 (2009).

[92] B. Block, P. Virnau, and T. Preis, Computer Physics Communications **181**, 1549 (2010).

[93] M. Weigel, Journal of Computational Physics **231**, 3064 (2012).

[94] Y. Lin, F. Wang, X. Zheng, H. Gao, and L. Zhang, Journal of computational Physics **237**, 224 (2013).

[95] P. L'ecuyer, Mathematics of Computation **68**, 249 (1999).

Year	**Reference**	**Method**	z
1981	Bausch	Theory	2.126
1984	Domany	Theory	2
1985	Williams	MC	2.13(3)
1987	Ito	MC	2.132 ± 0.008
1987	Tang	MC	2.17 ± 0.04
1988	Ito	MC	2.2
1988	Mori	MC	2.076 ± 0.005
1992	Stauffer	MC	2.18
1993	Dammann	Theory	2.183 ± 0.005
1993	Wang	Theory	2.207 ± 0.008
1993	Muenkel	MC	2.21 ± 0.03
1994	Grassberger	MC	2.172 ± 0.006
1995	Gropengiesser	MC	2.18 ± 0.02
1995	Li	MC	2.1337(41)
1996	Li	MC	2.143(5)
1996	Nightingale	MC	2.1665(12)
1997	Soares	MC	2.16 ± 0.03
1997	Wang	MC	2.168 ± 0.005
1997	Wang	MC	2.180 ± 0.009, TP
1997	Wang	MC	2.167 ± 0.008, hc
1997	Prudnikov	Theory	2.093
1998	Wang	Theory	2.2
2000	Nightingale	MC	2.1667 ± 0.0005
2005	Dunlavy	Experiment	2.09 ± 0.06
2006	Krinitsyin	Theory	2.0842 ± 0.0039
2007	Canet	Theory	2.16(1)
2007	Lei	MC	2.16
2008	Murase	MC	2.193(5)
2008	Murase	MC	2.198(4), hc
2008	Murase	MC	2.199(3), TP
2009	Nalimov	Theory	2.020 ± 0.045
2009	Nalimov	Theory	2.023 ± 0.053
2009	Nalimov	Theory	2.026 ± 0.055
2009	Nalimov	Theory	2.100 ± 0.089
2009	Nalimov	Theory	2.105 ± 0.084
2009	Nalimov	Theory	2.104 ± 0.080
2009	Nalimov	Theory	2.127 ± 0.089
2009	Nalimov	Theory	2.132 ± 0.084
2009	Nalimov	Theory	2.130 ± 0.080
2009	Nalimov	Theory	$2.037^{+0.033}_{-0.0}$
2009	Nalimov	Theory	$2.041^{+0.040}_{-0.0}$
2009	Nalimov	Theory	$2.042^{+0.041}_{-0.0}$
2017	Duclut	Theory	2.28
2017	Duclut	Theory	2.16
2017	Duclut	Theory	2.15
2017	Duclut	Theory	2.14
2022	Adzhemyan	Theory	2.14(2)

TABLE VI. All calculated exponents from the literature in two dimensions, to the best of our knowledge.

Year	**Reference**	**Method**	z
1987	Wansleben	MC	2.03 ± 0.04
1991	Wansleben	MC	2.04 ± 0.03
1992	Stauffer	MC	2.09
1993	Ito	MC	2.06(2)
1993	Muenkel	MC	2.08 ± 0.03
1994	Grassberger	MC	2.032 ± 0.004
1995	Gropengiesser	MC	2.04 ± 0.01
1997	Prudnikov	Theory	2.017
1999	Jaster	MC	2.042(6)
2000	Ito	MC	2.055(10)
2002	Livet	Experiment	2.2
2006	Krinitsyin	Theory	2.0237 ± 0.0055
2007	Canet	Theory	2.09(4)
2008	Murase	MC	2.065(25), bcc
2008	Murase	MC	2.057(25), fcc
2009	Nalimov	Theory	2.011 ± 0.012
2009	Nalimov	Theory	2.013 ± 0.012
2009	Nalimov	Theory	2.014 ± 0.011
2009	Nalimov	Theory	2.021 ± 0.006
2009	Nalimov	Theory	2.022 ± 0.005
2009	Nalimov	Theory	2.022 ± 0.005
2009	Nalimov	Theory	2.023 ± 0.006
2009	Nalimov	Theory	2.024 ± 0.005
2009	Nalimov	Theory	2.024 ± 0.005
2009	Nalimov	Theory	$2.013^{+0.011}_{-0.0}$
2009	Nalimov	Theory	$2.014^{+0.011}_{-0.0}$
2009	Nalimov	Theory	$2.014^{+0.011}_{-0.0}$
2010	Collura	MC	2.020(8)
2015	Livet	Experiment	2.28
2017	Niermann	Experiment	2.06
2017	Duclut	Theory	2.029
2017	Duclut	Theory	2.024
2017	Duclut	Theory	2.023
2017	Duclut	Theory	2.025
2017	Duclut	Theory	2.021
2017	Duclut	Theory	2.021
2018	Livet	Experiment	1.96(11)
2020	Hasenbusch	MC	2.0245(15)
2022	Adzheyman	Theory	2.0235(8)

TABLE VII. All calculated exponents from the literature in three dimensions, to the best of our knowledge.