

Phase transition in Random Circuit Sampling

Google Quantum AI and Collaborators

Quantum computers hold the promise of executing tasks beyond the capability of classical computers. Noise competes with coherent evolution and destroys long-range correlations, making it an outstanding challenge to fully leverage the computation power of near-term quantum processors. We report Random Circuit Sampling (RCS) experiments where we identify distinct phases driven by the interplay between quantum dynamics and noise. Using cross-entropy benchmarking, we observe phase boundaries which can define the computational complexity of noisy quantum evolution. We conclude by presenting an RCS experiment with 70 qubits at 24 cycles. We estimate the computational cost against improved classical methods and demonstrate that our experiment is beyond the capabilities of existing classical supercomputers.

The computational complexity of quantum systems arises from the exponential growth of the Hilbert space dimensions with system size. On near-term quantum processors whose practical complexity is limited by noise, random circuit sampling (RCS) has emerged as the most suitable candidate for a beyond-classical demonstration, as it allows for quantum correlation to spread at the maximized speed [1, 2]. In addition, RCS also relies on a minimal number of complexity theoretical assumptions compared to other proposals, such as related sampling problems [3, 4] or integer factorization, for overturning the Extended-Church Turing thesis in the noiseless case [1, 5–8].

The interplay between computational complexity and noise is highlighted by recent RCS experiments, starting with a 53-qubit Sycamore quantum processor in 2019 [9]. Ever since, similar experiments with expanded system sizes and reduced noise have been reported [10, 11], while classical algorithms have also advanced substantially [12–17]. This intensifying quantum-classical competition motivates two questions: does there exist well-defined boundaries for the region where the exponentially large Hilbert space is, in fact, leveraged by a noisy quantum processor? More importantly, can we establish an experimental observable that directly probes these boundaries?

In this work, we provide direct insight to these two questions using RCS on a second generation of Sycamore processors. We demonstrate that the interplay between quantum dynamics and noise can drive the system into distinct phases, whose boundaries are resolved using finite-size studies with cross-entropy benchmarking (XEB) [1, 9, 18, 19]. Reaching the desired phase of maximized complexity requires a noise rate per cycle below a critical threshold whose value is determined by the growth rate of quantum correlations. Finally, we report a 70-qubit RCS experiment and compare its results with calculations using tensor network contraction and matrix product states. After estimating the needed computation resources and achievable fidelity bound for improved classical methods, we conclude that our demonstration is firmly in the regime of beyond-classical quantum computation.

The structure of these phases is schematically illus-

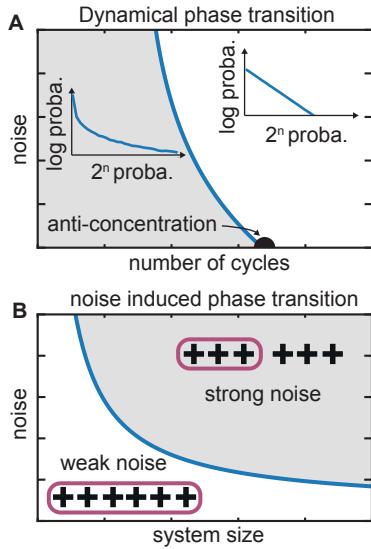


FIG. 1. Noise on Random Circuit Sampling: **A:** Phase transition between a concentrated output distribution of bitstrings from RCS at low number of cycles to a broad distribution. In a noiseless system, the phase transition between the two regimes is the anti-concentration point [20], in a noisy system, the transition point is lowered. **B:** At a sufficient number of cycles and for a finite size system, noise induces a phase transition from a regime where correlations extend to the full system to a regime where the system may be approximately represented by the product of multiple uncorrelated subsystems. In the strong noise regime, XEB on the full device also fails to give a faithful estimate of the underlying fidelity.

trated in Fig. 1. Driven by the circuit depth, the system first goes through a dynamic phase transition, where the output distribution is no longer concentrated in a fraction of bitstrings. This suggests that the system becomes sufficiently delocalized in the computational basis for linear XEB to become a good estimator of system fidelity (Fig. 1A). Noise drives the output towards the uniform distribution. As a consequence, the transition occurs at an earlier time, with a depth determined by the level of noise. Anticoncentration is a key ingredient of mathematical arguments on the complexity of simulating noiseless RCS [1, 5, 6, 20]. Nevertheless, this is a necessary

but not sufficient condition for global entanglement (see SM F) which maximizes computational cost.

The second is a transition driven by noise, specifically error rate per cycle $\epsilon \times n$, where ϵ is the error per gate and n is the number of qubits. As illustrated in Fig. 1B, the behavior of quantum correlations falls into two regimes: when the error rate per cycle is large, the wavefunction of the system may be approximately represented by multiple uncorrelated subsystems. This leaves the quantum system open to spoofing by classical algorithms that represent only part of the system at a time [9, 21–24]. In the regime where the error rate per cycle is sufficiently low, correlations span the entire system restoring its computational complexity. The boundary between these two phases is determined by the competition between the error rate per cycle and the convergence of the system to the ergodic state.

We find that XEB is a proper observable to resolve the aforementioned regimes experimentally. Specifically linear XEB is measured as

$$\text{XEB} = \langle 2^n p_{\text{sim}}(s) - 1 \rangle_{\text{experiment}}, \quad (1)$$

where n is the number of qubits, p_{sim} are ideal (simulated) probabilities and the average is over experimentally observed bitstrings. We measure XEB as a function of the number of cycles d for different system sizes to resolve the dynamical phase transition (Fig. 1A). The experimental results are shown in Fig. 2A and Fig. 2B for 1D and 2D systems, respectively. We find that XEB increases with system size for small d , where the system wavefunction is concentrated in a fraction of basis states. However, for large d , XEB decays exponentially and approximates the circuit fidelity. At intermediate depth we observe a critical crossing point where all the measured XEB curves intersect at a single point where the value of XEB is approximately independent of the system size. This behavior can be understood in the following way: at $d = 0$ the system is in a single basis state and $p_{\text{sim}}(s)$ is a delta function. Here XEB equals $2^n - 1$, i.e. increases with n exponentially. This exponential growth with n is preserved at short times with a depth dependence $\exp(ne^{-d})$ (see also Ref. [20]). At a later time the trend switches and it decays exponentially as F^d where $F \approx \exp(-\epsilon n)$ is the fidelity per cycle (i.e. the digital error model [9]). The phase transition between these two trends corresponds to the depth where the exponents e^{-d} and ϵd are approximately equal.

Having identified the minimum depth at which XEB approximates the system fidelity, we now formulate an experimental protocol for locating the transition between the strong and weak noise regimes (Fig. 1B). A conceptually simple setup that highlights the underlying physics for this transition is the so-called weak-link model, where two subsystems of size $n/2$ are coupled via an entangling gate applied every T cycles. In the limit where $T = \infty$, i.e. no weak link is applied, the subsystems are uncoupled and the overall system converges to a product state $\rho_A \otimes \rho_B$, where ρ_A (ρ_B) is the pure ergodic state of each

subsystem. Adding noise, we assume the so-called depolarizing channel noise model for the density matrix of each subsystem A/B : $F^{d/2}\rho_{A/B} + (1 - F^{d/2})I_{A/B}/2^{n/2}$, where I_A (I_B) is the identity matrix. Direct substitution of this density matrix into Eq. (1) gives $\text{XEB} = F^d + 2F^{d/2}$ using $\text{XEB} = 1$ for $\rho_{A/B}$ and $\text{XEB} = 0$ for $I_{A/B}/2^n$.

We now analyze the case of finite yet large T , such that each subsystem approaches the ergodic state in less than T cycles. In the average evolution of linear XEB over random circuits [2, 23] (see SM D), the application of each gate between the two systems entangles them with probability $1 - \lambda$. Entanglement evolves the subsystem ergodic state ρ_A (or ρ_B) towards the overall ergodic state ρ_{AB} . The probability λ depends on the entangling gate and is $1/4$ for the iSWAP-like gates employed in our experiment. Therefore, a simplified model for linear XEB is

$$\text{XEB} \approx 2\lambda^{d/T}F^{d/2} + F^d. \quad (2)$$

We probe this expected behavior by measuring XEB experimentally as a function of d , shown in Fig. 2C. Here we have employed a noise-injection protocol that effectively changes gate fidelities in our quantum circuits (see SM C2 for details) and show results corresponding to different noise levels. In the rest of the paper we use a discrete set of single-qubit gates chosen randomly from $Z^p X^{1/2} Z^{-p}$ with $p \in \{-1, -1/4, -1/2, \dots, 3/4\}$. We observe that in the weak noise regime, XEB converges to the expected fidelity of the entire system, F^d . This is because F is sufficiently high such that F^d dominates the contribution to XEB. On the other hand, we observe that XEB is significantly above F^d in the strong noise regime owing to the dominant contribution of $2\lambda^{d/T}F^{d/2}$ to XEB. These results are preliminary indications of the two different noise induced phases and exemplify the competition between the exponential decay of global correlations $\propto \epsilon n$, and the entangling rate between subsystems ($\propto 1/T$ in this example).

The transition between the two different noise induced phases is more clearly seen by fixing d to a few values past the dynamical phase transition in Fig. 1A. We then vary the effective noise level (i.e. F) and measure XEB at these fixed cycles (Fig. 2D). We observe XEB exhibits a nontrivial scaling distinct from F^d . In particular, we see that the rate of decay with respect to errors decreases at higher error rates. This is again consistent with the fact that $2\lambda^{d/T}F^{d/2}$ dominates at high errors.

To experimentally locate the critical value of error per cycle (or equivalently, F) where the dynamical exponent of XEB changes, we define a modified order parameter F^d/XEB , which asymptotes to a distinct value of 1 (0) in the weak (strong) noise regime. The transition between the two limits becomes a discontinuity when $d \rightarrow \infty$, indicating a phase transition for finite $\epsilon n \approx \kappa_c$, where the critical value κ_c may be a function of λ and T . In the transition region we can observe the finite size critical behavior where F^d/XEB is approximately a function

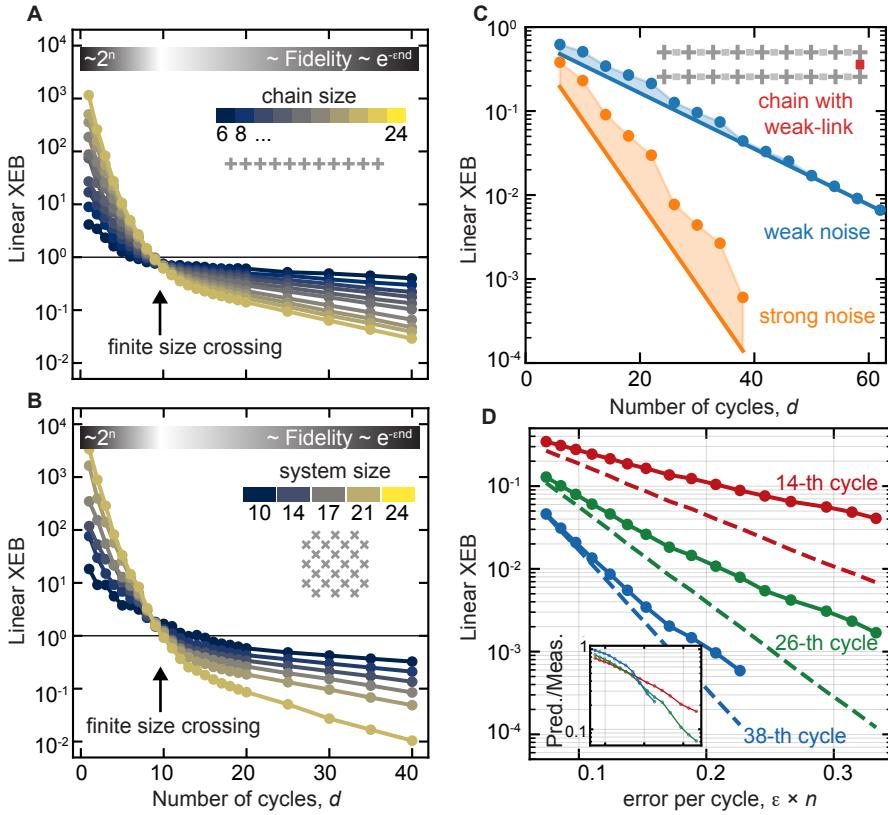


FIG. 2. At low depth, XEB grows with the size of the system. In a noiseless device, XEB will converge to 1 with the number of cycles. In the presence of noise XEB becomes an estimator of the system fidelity. In **A** and **B**, we observe experimentally a dynamical phase transition at a fixed number of cycles between these two regimes in 1D and 2D respectively. The random circuits here use Haar random single-qubit gates and an iSWAP-like gate as an entangler. In **C** and **D** we probe experimentally a noise induced phase transition using a weak-link model (see main text), where the weak link is applied every 12 cycles (discrete gate set, see main text). In **C** we show the two different regimes: in the weak noise regime, XEB converges to the fidelity, whereas in the strong noise regime, XEB remains higher than predicted by the digital error model. In **D**, we induce errors to scan the transition from one regime to the other. We show in the inset that there is a crossing point indicating a phase transition induced by noise.

of $(\epsilon n - \kappa_c)d$. This is revealed in the order parameter for different depths d crossing at a single point, as can be verified from Eq (2) and numerically for the circuits used in the experiment. The experimentally obtained F^d/XEB , shown in the inset of Fig. 2D, indeed manifests the expected critical behavior: for $\epsilon n \lesssim 0.17$, the order parameter increases as d increases whereas for $\epsilon n \gtrsim 0.17$, the order parameter decreases as d increases. At a critical point $\epsilon n \approx 0.17$, the data sets cross and the order parameter is approximately independent of d . We attribute the slight drift in the crossing point between different data sets to potential systematic errors in the experimental estimation of F .

We now explore the physical mechanism underlying the noise induced phase transition further. As discussed earlier, the period T in the weak-link model effectively controls the rate of coherent entanglement between the two subsystems and consequently the critical error rate per cycle associated with the transition. The results are

illustrated in Fig. 3A-C, where the T varies between values of 8, 12 and 18 cycles. For each value of T , we observe a finite-depth crossing in the noise dependence of F^d/XEB , rendering the critical noise rate $n\epsilon$ which decreases as we increase the value of T . This result is intuitively expected: by increasing the period of the weak link, we reduce the entanglement generation rate between the two subsystems, making the entire system more susceptible to noise induced correlation localization. To construct the corresponding phase diagram, we extract the value of critical noise rate and plot them against $1/T$ - the link frequency (red dots), as shown in Fig. 3D. They are in good agreement with numerical simulations with noise (blue dots), marking the phase boundary between the weak and strong noise regimes. When comparing with the functional form $n\epsilon \simeq 4/T \log 2$ predicted by the analytical weak-link model, we observe appreciable deviations when link frequency is approaching $1/2$, which corresponds to the regular 1D chain. The deviation re-

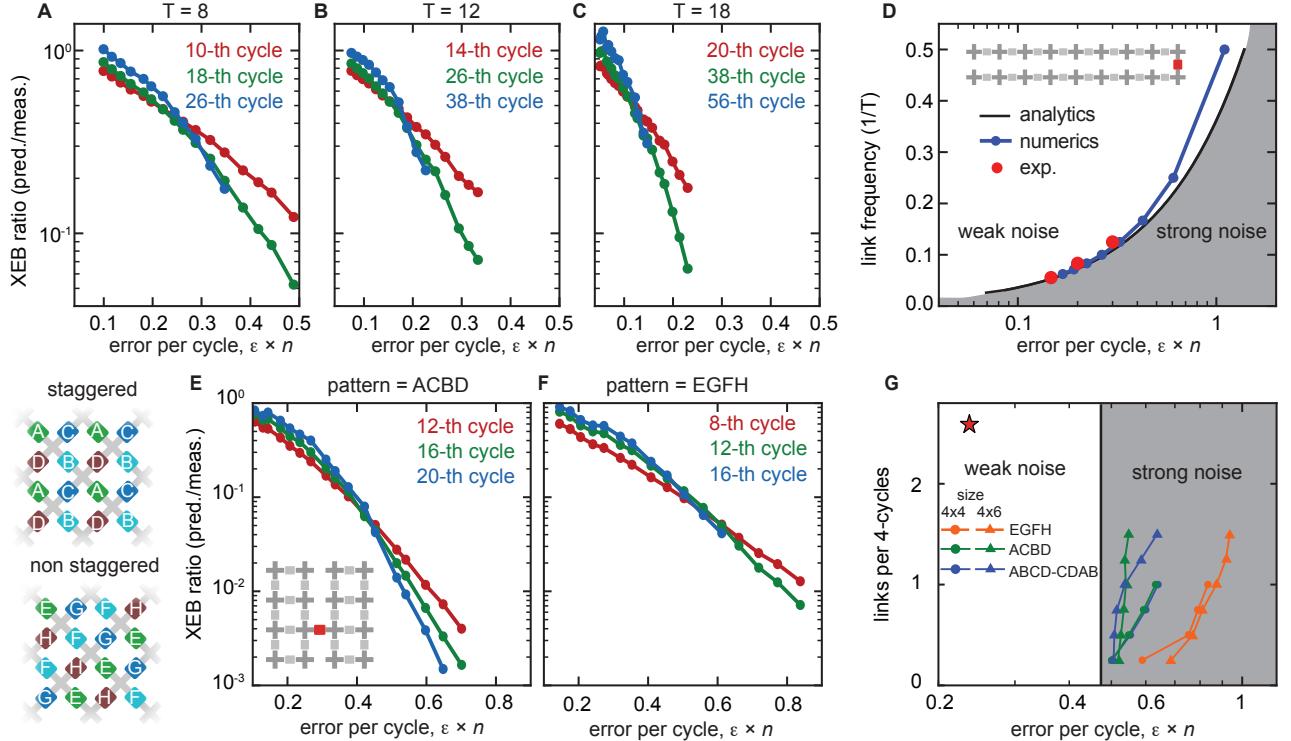


FIG. 3. Noise Induced Phase Transition: **A, B, C:** Experimental noise induced phase transition as a function of the error per cycle for several periods T of the weak-link model described in Fig. 2 (discrete gate set). As the period increases, the critical value of noise or error per cycle gets lower. **D:** Phase diagram of the transition with analytical, numerical and experimental data. The experimental data is extracted from the crossing of the largest depth scan. **E, F:** Experimental transition in 2D with different patterns: staggered ACBD and non-staggered EGFH respectively (discrete gate set). **G:** Numerical phase diagram of the 2D phase transition. We show the critical point for different sizes and patterns, including the pattern used for the beyond-classical RCS experiment presented in this manuscript (staggered ABCD-CDAB, see Fig. 4). The qubits are arranged as in the inset of panel E. For fixed size we vary the number of bridges (such as the red coupler in panel E) up to the point when all bridges are applied (4 and 6 for the 4×4 and 4×6 systems, respectively), denoted as links per 4-cycles in the panel G. For all the patterns, we delimit a pessimistic critical error rate of 0.47 error per cycle to separate the region of strong noise where XEB fails to characterize the underlying fidelity and global correlations are subdominant. The experiment of Fig. 4 is represented by a red star and is well within the weak noise regime.

flects that the interaction between the correlation length and noise is not fully captured in the simple analytical model. [25]

With the ultimate goal of demonstrating and verifying the beyond-classical performance for our 70-qubit device, it is critical to construct a similar phase diagram for the full 2D structure to ensure that our system is in the required weak noise regime, which in turn guarantees XEB is a proper estimate of the fidelity. However, performing the same experiment and analysis at the level of 70 qubits is classically intractable to begin with. Instead, we performed investigations at reduced system sizes, combining experiments with the numerical analysis to give a proper bound that is applicable to larger sizes. The experimental results are shown in Fig. 3E-F for a 4×4 square grid of qubits and two different circuit structures, whereby the two-qubit gates are applied either in a staggered (Fig. 3E) or a non-staggered (Fig. 3F) fashion. Similarly to 1D, the 16-qubit system is divided into two halves that are con-

nected by a single iSWAP-like gate applied every 4 cycles. For both circuit structures, we observe a similar crossing between F^d /XEB measured at three different cycles, with a higher value of $n\epsilon$ observed for the non-staggered patterns.

We performed further investigations by numerically evaluating critical noise rates for systems of different sizes and circuit structures, including both the staggered and non-staggered patterns and the ABCD-CDAB pattern used in the 2019 and the current beyond-classical demonstrations. As the illustrated in Fig. 3G, 2D gate patterns introduce qualitatively different behavior for quantum correlations under noise. Compared with 1D, the critical noise rates in 2D systems demonstrate a much weaker dependence on the applied link frequency, assuming a narrow range of $n\epsilon$ between 0.5 to 0.6. This reduced sensitivity comes from the fact that in 2D, the dynamics are dominated by the bulk effect within each subsystem and less by the the weak link itself. This weak dependence is

also observed on the system size. When being increased from 4×4 (dots) to 4×6 (triangles), we found that $n\epsilon$ remains within the same range. The suggested weak dependence provided us the confidence to conclude a lower bound to separate the weak noise regime from the strong noise regime. As the solid black line shown in Fig. 3G, we identified the lowest transition point observed in the weak-link model and use it as the empirical boundary for the noise induced phase transition. With the phase diagram constructed, we compare it with our 70-qubit RCS experiment that we will present next. It is evident that our system falls well within the weak noise regime, satisfying the requirement to fully utilize the computational capacity of the noisy quantum processors.

Finally, we show in Fig. 4 evidence for the demonstration of beyond-classical RCS by performing the experiment on a 70-qubits Sycamore chip. The random circuits follow the same 2-dimensional pattern as Ref. [9] ABCD-CDAB, where single-qubit gates are chosen randomly from $Z^p X^{1/2} Z^{-p}$ with $p \in \{-1, -1/4, -1/2, \dots, 3/4\}$. We show in SM B the fidelity of the elementary operations of the random circuit. On average, we achieve a single-qubit Pauli error rate of $1.1(0.6) \times 10^{-3}$, a readout fidelity of $1.3(0.4) \times 10^{-2}$, and a dressed two-qubit Pauli error rate of $6.7(2.5) \times 10^{-3}$ (simultaneous two-qubit gates and single-qubit gates), corresponding to an intrinsic two-qubit simultaneous error rate of $4(2) \times 10^{-3}$. We validate the digital error model by looking at patched variations of the random circuit (see inset in Fig. 4A), where slices of two-qubit gates have been removed, creating patched circuits for which each patch XEB can be verified at modest computational cost. The total fidelity is then the product of the patch fidelities. The difference between the two-patch and the three-patch fidelities is explained by the larger error rate of the two-qubit gates compared to the idling of the qubits for which two-qubit gates have been removed. Computing XEB over full circuits is currently an intractable classical task. We thus give an estimate of the fidelity obtained after 24 cycles –marked by a star in Fig. 4A– using the discrete error model. For this data point, we have collected 70 million sample bitstrings for a single circuit, for which we estimate a fidelity above 0.1%. In SM C1 we report fidelities for the phased-matched version of this experiment.

We now study the two main numerical methods used to perform RCS on classical hardware. The first method is tensor network contraction [12–17, 26]: Ref. [16] showed sampling from the largest circuits of Ref. [9] in 15 hours using 512 GPUs and Ref. [26] computed the corresponding XEB. The second method is based on Matrix Product States (MPS), a popular tensor network variational representation of 1D quantum states with limited entanglement [27, 28]. Contrary to the claim of Ref. [29], we find that given current supercomputer memory constraints this method fails to reach a fidelity comparable to the experimental one, and furthermore offer worse performance than tensor network contraction.

We report improvements in tensor network contrac-

Exp.	1 amp.	1 million noisy samples		
	FLOPs	FLOPs	XEB fid.	Time
SYC-53 [9]	$6.44 \cdot 10^{17}$	$2.60 \cdot 10^{17}$	$2.24 \cdot 10^{-3}$	6.18 s
ZCZ-56 [10]	$6.24 \cdot 10^{19}$	$6.40 \cdot 10^{19}$	$6.62 \cdot 10^{-4}$	25.3 min
ZCZ-60 [11]	$1.32 \cdot 10^{21}$	$1.41 \cdot 10^{23}$	$3.66 \cdot 10^{-4}$	38.7 days
This work	$4.74 \cdot 10^{23}$	$6.27 \cdot 10^{25}$	$1.68 \cdot 10^{-3}$	47.2 yr

TABLE I. **Estimated computational cost of simulation:** The second column shows the number of FLOPS needed for the computation of a single output amplitude from the random circuit assuming no memory constraints. This serves as a lower bound to the computational hardness of the simulation of sampling from each circuit. The last three columns refer to the cost of the simulation of noisy sampling of 1 million bitstrings. We use the specifications of Frontier for our estimates, with 1.685×10^{18} FLOPS of theoretical peak performance spread across GPUs with 128 GB of RAM each. We assume a 20% FLOP efficiency [14–16] and account for the low target fidelity of the simulation in the computational cost [14, 15, 21, 30].

tion techniques, which result in lower estimated computational costs for simulated RCS (see SM E). In Fig. 4B we show the FLOP count (the number of multiplications and additions) as a function of number of qubits and cycles required to compute a single amplitude at the output of a random circuit without memory constraints. This serves as a proxy lower bound for the hardness of both sampling and verification. For a fixed number of qubits and increasing depth, there is a crossover in the scaling of the computational cost from exponential to linear. Given a noisy experimental setup, this implies an optimal depth for the trade off between computational hardness and fidelity: beyond the crossover, fidelity decreases faster than the hardness increases. The crossover depth is consistent with a scaling \sqrt{n} , as indicated with a dashed line. Note that this is a stronger requirement than the anti-concentrated output distribution (Fig. 1A), and is related to the depth at which “typical” entanglement is achieved (see SM F). At 70 qubits, 24 cycles is deep enough to saturate the exponential growth of computational cost. The inset of Fig. 4A shows the growth in computational hardness (FLOP count) over the last few years.

A practical estimate of the computational resources needed to simulate RCS needs to take into account the finite FLOPS computational efficiency of a supercomputer as well as its memory constraints and other limitations such as finite bandwidth. Table I shows estimates of the runtime for the approximate simulation of the largest instances of RCS from Refs. [9–11] and the $m = 24$ instance of the current work when using the state-of-the-art methods discussed in SM E. In these estimates, we consider sampling 1 million uncorrelated bitstrings at a fidelity similar to that of the experiment using the current top-performing supercomputer, Frontier. This requires the computation of 10 million approximate probability am-

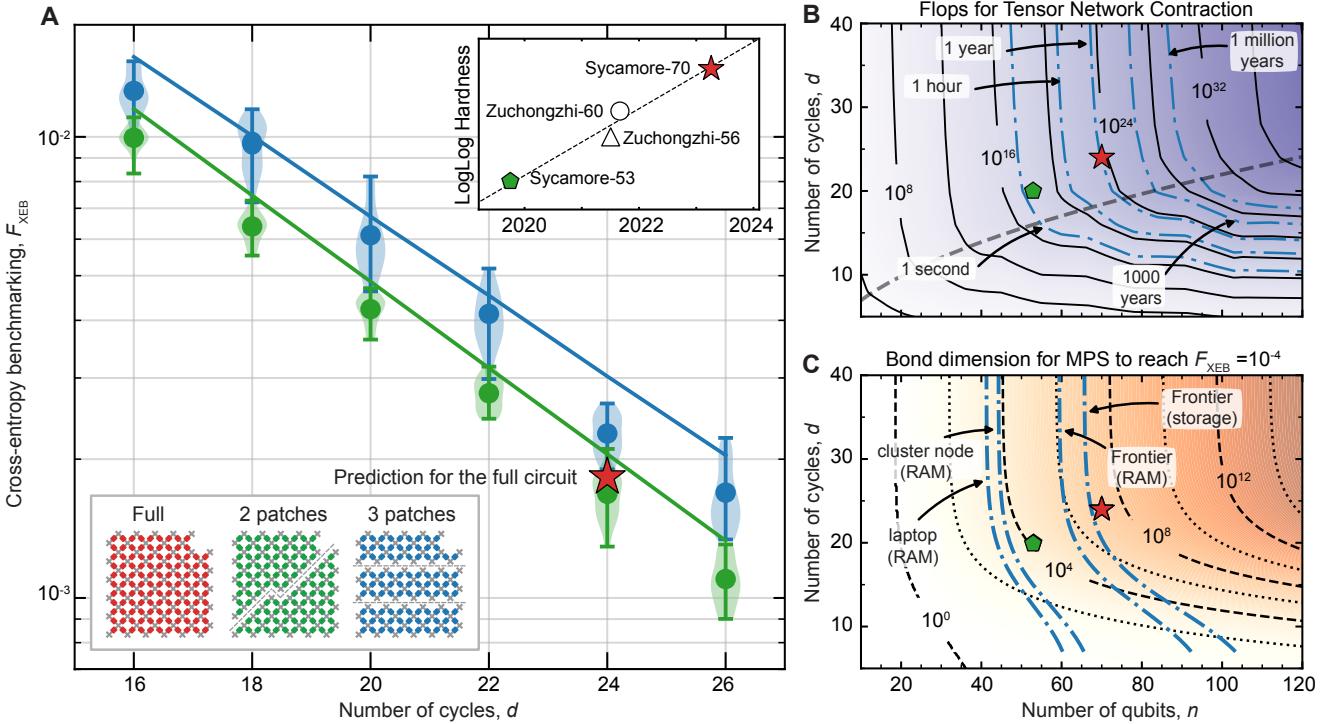


FIG. 4. Demonstration of quantum advantage **A:** Verification of RCS with logarithmic XEB. The full device is divided into two (green) or three (blue) patches to allow for XEB fidelity estimation with modest computational cost. We use the discrete gate set of single-qubit gates chosen randomly from $Z^p X^{1/2} Z^{-p}$ with $p \in \{-1, -1/4, -1/2, \dots, 3/4\}$. For each depth, 20 circuit instances are sampled with 100 thousand shots each. The solid lines indicate the estimated XEB from the digital error model. The star represents the estimated XEB of a single random circuit on the full processor sampled 70 million times. In the inset we show the evolution of the computational hardness of the RCS experiments, which is not inconsistent with a doubly-exponential growth. As a working definition of hardness we consider the estimated FLOPS –number of multiplications and additions– needed to compute the probability of a single bitstring assuming no memory constraints. **B:** Estimated hardness as a function of the number of qubits and the number of cycles for a set of circuits over layouts similar to Sycamore. Hardness serves as a proxy for the classical computational cost of RCS. We also indicate with the contour lines the computation time from the FLOP count if Frontier –the current largest supercomputer– ran at peak performance and without memory constraints. **C:** Bond dimension needed to achieve a finite fidelity of 10^{-4} with an MPS related method. We use the bond dimension (and therefore memory) as an indicator of computational cost. We show that the current experiment is well beyond the memory capacity of Frontier.

plitudes of uncorrelated bitstrings using rejection sampling [21].

Let us shift our attention to MPS simulation methods. The amount of entanglement represented by an MPS (and the corresponding computational cost) is controlled by the so-called bond dimension χ . Note that the required FLOPs scale as $O(2^n \chi)$ if we represent the state with two equal size tensors. We focus on partitioning the system in two halves in order to find a lower bound to the bond dimension χ required to achieve a given fidelity for the simulation of RCS using MPS methods. We give in SM F a precise method to compute this lower bound, and pinpoint the depth of a sharp transition to the “typical” (quasi-maximum) entanglement (see also Ref. [31]). We also show that linear XEB remains a good estimator of fidelity in this case [32].

In order to be of any practical use, χ must be much smaller than the Hilbert space dimension of the halves,

with $\chi \lesssim 10^3$ for most realistic implementations. Fig. 4C shows the required χ to reach a fidelity of $F \approx 10^{-4}$, as a function of the number of qubits and cycles. The reported memory footprint is the required memory to store two complex arrays of sizes $2^{n/2} \times \chi$. For 70 qubits and 24 cycles, the bond dimension χ required is of the order of 10^7 (with 35 qubits in each half), which is well beyond the capacity of Frontier.

In conclusion, we present a new RCS experiment with an estimated fidelity of $1.7 \cdot 10^{-3}$ at 70 qubits and 24 cycles, representing an increase of circuit volume of about 60% for the same fidelity. Looking forward, despite the successes of RCS achieved so far, finding practical applications for near-term noisy quantum processors still remains as an outstanding challenge. The experiments reported here provide direct insights on how quantum dynamics interacts with noise. The observed phase boundaries lay out quantitative guidance to the

regimes where noisy quantum devices can properly leverage their computational power. The fact that global correlations dominate XEB in the weak noise phase protects RCS against “spoofing” attacks, in contrast to Boson-Sampling [3], where all known metrics for recent experiments [33–35] are dominated by local correlations [36]. These are the regimes where future applications should be designed. Certified randomness generation [37–39] could be a promising candidate for such an application (see SM G).

Author contribution:

Y. Chen and S. Boixo led the overall project. A. Morvan and X. Mi performed the experiment. A. Bengtsson contributed to readout developments. X. Mi and P. V. Klimov contributed to gate developments. B. Villalonga developed and ran the tensor network contraction simulations and optimizations. S. Mandrà developed and ran the MPS simulations. A. Morvan, Z. Chen, S. Hong, C. Erickson, P. V. Klimov and I. K. Drozdov contributed to large-system calibration and stability

Google Quantum AI and Collaborators

A. Morvan^{1,‡}, B. Villalonga^{1,‡}, X. Mi^{1,‡}, S. Mandrà^{1,2,3,‡}, A. Bengtsson¹, P. V. Klimov¹, Z. Chen¹, S. Hong¹, C. Erickson¹, I. K. Drozdov^{1,4}, J. Chau¹, G. Laun¹, R. Movassagh¹, A. Asfaw¹, L. T.A.N. Brandão⁵, R. Peralta⁵, D. Abanin¹, R. Acharya¹, R. Allen¹, T. I. Andersen¹, K. Anderson¹, M. Ansmann¹, F. Arute¹, K. Arya¹, J. Atalaya¹, J. C. Bardin^{1,6}, A. Bilmes¹, G. Bortoli¹, A. Bourassa¹, J. Bovaard¹, L. Brill¹, M. Broughton¹, B. B. Buckley¹, D. A. Buell¹, T. Burger¹, B. Burkett¹, N. Bushnell¹, J. Campero¹, H.-S. Chang¹, B. Chiaro¹, D. Chik¹, C. Chou¹, J. Cogan¹, R. Collins¹, P. Conner¹, W. Courtney¹, A. L. Crook¹, B. Curtin¹, D. M. Debroy¹, A. Del Toro Barba¹, S. Demura¹, A. Di Paolo¹, A. Dunsworth¹, L. Faoro¹, E. Farhi¹, R. Fatemi¹, V. S. Ferreira¹, L. Flores Burgos¹, E. Forati¹, A. G. Fowler¹, B. Foxen¹, G. Garcia¹, É. Genois¹, W. Giang¹, C. Gidney¹, D. Gilboa¹, M. Giustina¹, R. Gosula¹, A. Grajales Dau¹, J. A. Gross¹, S. Habegger¹, M. C. Hamilton^{1,7}, M. Hansen¹, M. P. Harrigan¹, S. D. Harrington¹, P. Heu¹, M. R. Hoffmann¹, T. Huang¹, A. Huff¹, W. J. Huggins¹, L. B. Ioffe¹, S. V. Isakov¹, J. Iveland¹, E. Jeffrey¹, Z. Jiang¹, C. Jones¹, P. Juhas¹, D. Kafri¹, T. Khattar¹, M. Khezri¹, M. Kieferová^{1,8}, S. Kim¹, A. Kitaev¹, A. R. Klots¹, A. N. Korotkov^{1,9}, F. Kostritsa¹, J. M. Kreikebaum¹, D. Landhuis¹, P. Laptev¹, K.-M. Lau¹, L. Laws¹, J. Lee^{1,10}, K. W. Lee¹, Y. D. Lensky¹, B. J. Lester¹, A. T. Lill¹, W. Liu¹, A. Locharla¹, F. D. Malone¹, O. Martin¹, S. Martin¹, J. R. McClean¹, M. McEwen¹, K. C. Miao¹, A. Mieszala¹, S. Montazeri¹, W. Mruczkiewicz¹, O. Naaman¹, M. Neeley¹, C. Neill¹, A. Nersisyan¹, M. Newman¹, J. H. Ng¹, A. Nguyen¹, M. Nguyen¹, M. Yuezhen Niu¹, T. E. O’Brien¹, S. Omonije¹, A. Opremcak¹, A. Petukhov¹, R. Potter¹, L. P. Pryadko¹¹, C. Quintana¹, D. M. Rhodes¹, C. Rocque¹, P. Roushan¹, N. C. Rubin¹, N. Saei¹, D. Sank¹, K. Sankaragomathi¹, K. J. Satzinger¹, H. F. Schurkus¹, C. Schuster¹, M. J. Shearn¹, A. Shorter¹, N. Shutty¹, V. Shvarts¹, V. Sivak¹, J. Skrzyni¹, W. C. Smith¹, R. D. Somma¹, G. Sterling¹, D. Strain¹, M. Szalay¹, D. Thor¹, A. Torres¹, G. Vidal¹, C. Vollgraff Heidweiller¹, T. White¹, B. W. K. Woo¹, C. Xing¹, Z. J. Yao¹, P. Yeh¹, J. Yoo¹, G. Young¹, A. Zalcman¹, Y. Zhang¹, N. Zhu¹, N. Zobrist¹, E. G. Rieffel², R. Biswas², R. Babbush¹, D. Bacon¹, J. Hilton¹, E. Lucero¹, H. Neven¹, A. Megrant¹, J. Kelly¹, I. Aleiner¹, V. Smelyanskiy¹, K. Kechedzhi^{1,§}, Y. Chen^{1,§}, S. Boixo^{1,§},

¹ Google Research

² Quantum Artificial Intelligence Laboratory, NASA Ames Research Center, Moffett Field, California 94035, USA

³ KBR, 601 Jefferson St., Houston, TX 77002, USA

⁴ Department of Physics, University of Connecticut, Storrs, CT

⁵ National Institute of Standards and Technology (NIST), USA

⁶ Department of Electrical and Computer Engineering, University of Massachusetts, Amherst, MA

⁷ Department of Electrical and Computer Engineering, Auburn University, Auburn, AL

⁸ QSI, Faculty of Engineering and Information Technology, University of Technology Sydney, NSW, Australia

⁹ Department of Electrical and Computer Engineering, University of California, Riverside, CA

¹⁰ Department of Chemistry, Harvard University, Boston, NY

¹¹ Department of Physics and Astronomy, University of California, Riverside, CA

[‡] These authors contributed equally to this work.

[§] Corresponding author: boixo@google.com

improvements. I. Aleiner and K. Kechedzhi developed theories and performed numerical simulations of phase transitions. J. Chau, G. Laun, R. Movassagh, L. T.A.N. Brandão and R. Peralta worked on certified randomness. A. Asfaw provided technical program management to the project. All authors contributed to building the hardware and software infrastructures and writing the manuscript.

Acknowledgment:

S. Mandrà is partially supported by the Prime Contract No. 80ARC020D0010 with the NASA Ames Research Center and acknowledges funding from DARPA under IAA 8839. We would like to acknowledge Carl Miller for discussions on certified randomness and Kevin Jeffery Sung for his work on randomness extractors.

Competing interests

The authors declare no competing interests.

[§] Corresponding author: bryanchen@google.com

[§] Corresponding author: kostyantyn@google.com

-
- [1] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, M. J. Bremner, J. M. Martinis, and H. Neven, Characterizing quantum supremacy in near-term devices, *Nature Physics* **14**, 595 (2018).
- [2] X. Mi, P. Roushan, C. Quintana, S. Mandrà, J. Marshall, C. Neill, F. Arute, K. Arya, J. Atalaya, R. Babbush, *et al.*, Information scrambling in quantum circuits, *Science* **374**, 1479 (2021).
- [3] S. Aaronson and A. Arkhipov, The computational complexity of linear optics, in *Proceedings of the forty-third annual ACM symposium on Theory of computing* (2011) pp. 333–342.
- [4] M. J. Bremner, A. Montanaro, and D. J. Shepherd, Average-case complexity versus approximate simulation of commuting quantum computations, *Physical review letters* **117**, 080501 (2016).
- [5] A. Bouland, B. Fefferman, C. Nirkhe, and U. Vazirani, On the complexity and verification of quantum random circuit sampling, *Nature Physics* **15**, 159 (2019).
- [6] R. Movassagh, Quantum supremacy and random circuits, arXiv preprint arXiv:1909.06210 (2019).
- [7] Y. Kondo, R. Mori, and R. Movassagh, Quantum supremacy and hardness of estimating output probabilities of quantum circuits, in *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, 2022) pp. 1296–1307.
- [8] A. Bouland, B. Fefferman, Z. Landau, and Y. Liu, Noise and the frontier of quantum supremacy, in *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, 2022) pp. 1308–1317.
- [9] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M. P. Harrigan, M. J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T. S. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P. V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandrà, J. R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michelsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Y. Niu, E. Ostby, A. Petukhov, J. C. Platt, C. Quintana, E. G. Rieffel, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, K. J. Sung, M. D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven, and J. M. Martinis, Quantum supremacy using a programmable superconducting processor, *Nature* **574**, 505 (2019).
- [10] Y. Wu, W.-S. Bao, S. Cao, F. Chen, M.-C. Chen, X. Chen, T.-H. Chung, H. Deng, Y. Du, D. Fan, M. Gong, C. Guo, C. Guo, S. Guo, L. Han, L. Hong, H.-L. Huang, Y.-H. Huo, L. Li, N. Li, S. Li, Y. Li, F. Liang, C. Lin, J. Lin, H. Qian, D. Qiao, H. Rong, H. Su, L. Sun, L. Wang, S. Wang, D. Wu, Y. Xu, K. Yan, W. Yang, Y. Yang, Y. Ye, J. Yin, C. Ying, J. Yu, C. Zha, C. Zhang, K. Zhang, Y. Zhang, H. Zhao, Y. Zhao, L. Zhou, C.-Y. Lu, C.-Z. Peng, X. Zhu, and J.-W. Pan, Strong quantum computational advantage using a superconducting quantum processor, *Phys. Rev. Lett.* **127**, 180501 (2021).
- [11] Q. Zhu, S. Cao, F. Chen, M.-C. Chen, X. Chen, T.-H. Chung, H. Deng, Y. Du, D. Fan, M. Gong, C. Guo, C. Guo, S. Guo, L. Han, L. Hong, H.-L. Huang, Y.-H. Huo, L. Li, N. Li, S. Li, Y. Li, F. Liang, C. Lin, J. Lin, H. Qian, D. Qiao, H. Rong, H. Su, L. Sun, L. Wang, S. Wang, D. Wu, Y. Wu, Y. Xu, K. Yan, W. Yang, Y. Yang, Y. Ye, J. Yin, C. Ying, J. Yu, C. Zha, C. Zhang, H. Zhang, K. Zhang, Y. Zhang, H. Zhao, Y. Zhao, L. Zhou, C.-Y. Lu, C.-Z. Peng, X. Zhu, and J.-W. Pan, Quantum computational advantage via 60-qubit 24-cycle random circuit sampling, *Science Bulletin* **67**, 240 (2022).
- [12] I. L. Markov and Y. Shi, Simulating quantum computation by contracting tensor networks, *SIAM Journal on Computing* **38**, 963 (2008).
- [13] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, and H. Neven, Simulation of low-depth quantum circuits as complex undirected graphical models, arXiv preprint arXiv:1712.05384 (2017).
- [14] J. Gray and G. K. Chan, Hyper-optimized compressed contraction of tensor networks with arbitrary geometry, arXiv:2206.07044 (2022).
- [15] C. Huang, F. Zhang, M. Newman, J. Cai, X. Gao, Z. Tian, J. Wu, H. Xu, H. Yu, B. Yuan, *et al.*, Classical simulation of quantum supremacy circuits, arXiv preprint arXiv:2005.06787 (2020).
- [16] F. Pan, K. Chen, and P. Zhang, Solving the sampling problem of the sycamore quantum circuits, *Physical Review Letters* **129**, 090502 (2022).
- [17] G. Kalachev, P. Panteleev, P. Zhou, and M.-H. Yung, Classical sampling of random quantum circuits with bounded fidelity, arXiv preprint arXiv:2112.15083 (2021).
- [18] C. Neill, P. Roushan, K. Kechedzhi, S. Boixo, S. V. Isakov, V. Smelyanskiy, A. Megrant, B. Chiaro, A. Dunsworth, K. Arya, *et al.*, A blueprint for demonstrating quantum supremacy with superconducting qubits, *Science* **360**, 195 (2018).
- [19] Y. Liu, M. Otten, R. Bassirianjahromi, L. Jiang, and B. Fefferman, Benchmarking near-term quantum computers via random circuit sampling, arXiv preprint arXiv:2105.05232 (2021).
- [20] A. M. Dalzell, N. Hunter-Jones, and F. G. S. L. Brandão, Random quantum circuits anticoncentrate in log depth, *PRX Quantum* **3**, 010333 (2022).
- [21] I. L. Markov, A. Fatima, S. V. Isakov, and S. Boixo, Quantum supremacy is both closer and farther than it appears, arXiv preprint arXiv:1807.10749 (2018).
- [22] A. Zlokapa, S. Boixo, and D. Lidar, Boundaries of quantum supremacy via random circuit sampling, arXiv preprint arXiv:2005.02464 (2020).

- [23] X. Gao, M. Kalinowski, C.-N. Chou, M. D. Lukin, B. Barak, and S. Choi, Limitations of linear cross-entropy as a measure for quantum advantage, arXiv preprint arXiv:2112.01657 (2021).
- [24] D. Aharonov, X. Gao, Z. Landau, Y. Liu, and U. Vazirani, A polynomial-time classical algorithm for noisy random circuit sampling, arXiv preprint arXiv:2211.03999 (2022).
- [25] Note that the transition discussed here is qualitatively different from the quantum to classical transition discussed in Ref. 40. The transition discussed here is a competition between the finite rate of convergence to the overall ergodic state and the fidelity per cycle. The transition in Ref. 40 is a competition between local interactions and the error rate per qubit.
- [26] Y. Liu, Y. Chen, C. Guo, J. Song, X. Shi, L. Gan, W. Wu, W. Wu, H. Fu, X. Liu, *et al.*, Validating quantum-supremacy experiments with exact and fast tensor network contraction, arXiv preprint arXiv:2212.04749 (2022).
- [27] S. R. White, Density-matrix algorithms for quantum renormalization groups, *Physical review b* **48**, 10345 (1993).
- [28] G. Vidal, Efficient classical simulation of slightly entangled quantum computations, *Physical review letters* **91**, 147902 (2003).
- [29] T. Ayral, T. Louvet, Y. Zhou, C. Lambert, E. M. Stoudenmire, and X. Waintal, A density-matrix renormalisation group algorithm for simulating quantum circuits with a finite fidelity, arXiv:2207.05612 (2022).
- [30] B. Villalonga, S. Boixo, B. Nelson, C. Henze, E. Rieffel, R. Biswas, and S. Mandrà, A flexible high-performance simulator for verifying and benchmarking quantum circuits implemented on real hardware, *npj Quantum Information* **5**, 86 (2019).
- [31] R. Oliveira, O. Dahlsten, and M. Plenio, Generic entanglement can be generated efficiently, *Physical review letters* **98**, 130502 (2007).
- [32] Ref. [29] claims that using MPS methods the linear XEB scales as the square root of the fidelity, which contradicts our findings. This is because a) at low depth they compute XEB before the anti-concentration point and b) at high depth they plot the absolute value of the linear XEB (instead of the linear XEB itself).
- [33] 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, *et al.*, Quantum computational advantage using photons, *Science* **370**, 1460 (2020).
- [34] H.-S. Zhong, Y.-H. Deng, J. Qin, H. Wang, M.-C. Chen, L.-C. Peng, Y.-H. Luo, D. Wu, S.-Q. Gong, H. Su, 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, J. J. Renema, C.-Y. Lu, and J.-W. Pan, Phase-programmable gaussian boson sampling using stimulated squeezed light, *Phys. Rev. Lett.* **127**, 180502 (2021).
- [35] L. S. Madsen, F. Laudenbach, M. F. Askarani, F. Rortais, T. Vincent, J. F. F. Bulmer, F. M. Miatto, L. Neuhaus, L. G. Helt, M. J. Collins, A. E. Lita, T. Gerrits, S. W. Nam, V. D. Vaidya, M. Menotti, I. Dhand, Z. Vernon, N. Quesada, and J. Lavoie, Quantum computational advantage with a programmable photonic processor, *Nature* **606**, 75 (2022).
- [36] B. Villalonga, M. Y. Niu, L. Li, H. Neven, J. C. Platt, V. N. Smelyanskiy, and S. Boixo, Efficient approximation of experimental gaussian boson sampling, arXiv preprint arXiv:2109.11525 (2021).
- [37] S. Aaronson, Certified randomness from quantum supremacy, Talk at CRYPTO 2018 (2018).
- [38] R. Bassirian, A. Bouland, B. Fefferman, S. Gunn, and A. Tal, On certified randomness from quantum advantage experiments, arXiv preprint arXiv:2111.14846 (2021).
- [39] S. Aaronson and S.-H. Hung, Certified randomness from quantum supremacy, arXiv preprint arXiv:2303.01625 (2023).
- [40] D. Aharonov, Quantum to classical phase transition in noisy quantum computers, *Physical Review A* **62**, 10.1103/physreva.62.062311 (2000).

Supplement to Phase transition in Random Circuit Sampling

Google Quantum AI and Collaborators

CONTENTS

A. General RCS with XEB theory	1	c. A faster randomness extractor using HMAC	26
B. Device characterization and benchmarking	2	References	28
1. Gate Optimization	2		
2. Benchmarking of gates and readout	4		
C. Additional experimental data	4	Appendix A: General RCS with XEB theory	
1. Phase-matching RCS experiment	4	We show in this appendix that, under quite general	
2. Adding noise	6	conditions (see Eq. (A10)), the effect of noise in XEB	
3. Noise phase transition extended data	6	can be approximated as a globally depolarizing channel.	
D. Linear XEB via population dynamics	6	We use this to write an XEB estimator from any smooth	
1. Population dynamics for the uniformly random	6	and O(1) function $f(p_j)$ of the ideal probabilities p_j .	
single qubit gate ensemble			
2. Convergence of population dynamics to	8	It is non-trivial but true that the density of probabilities	
Porter-Thomas	8	from a Haar random pure quantum state is uniform	
3. Weak-link model analytical solution	9	in the probability simplex [1–3]	
4. Numerical analysis of the phase transitions	9		
E. Simulation of random circuit sampling using	11	$dP(p_1, \dots, p_D) = (N - 1)! dp_1 \cdots dp_D ,$	(A1)
tensor network contraction			
F. Bounds to approximate tensor representations	11	where $D = 2^n$ for n qubits. The corresponding marginal	
1. Fidelity for Haar random states	12	distribution for any one probability p_j is the Porter-	
2. Fidelity bound for arbitrary states	12	Thomas (exponential or beta) distribution [4]. That is,	
3. Open and close simulations using approximate	13	for all j we have	
tensor representations	13		
4. XEB for approximate tensor representations	14	$dP(p_j) = (D - 1)(1 - p_j)^{D-2} dp_j$	(A2)
5. Quantifying entanglement with Clifford	17	$\rightarrow D e^{-Dp_j} dp_j .$	(A3)
circuits	17		
6. Reduced purity and distribution of singular	18	In the previous expression the bitstring index j is fixed,	
values	18	and the distribution is over quantum states sampled uni-	
7. Bounding the approximate tensor	18	formly in Hilbert space (Haar measure).	
representation performance for close	18	One can sample a vector of the probabilities corre-	
simulations		sponding to a Haar random pure quantum state by	
G. Client-certified randomness generation with RCS	19	sampling D probabilities according to the distribution	
1. Entropy estimation	20	of Eq. (A3), and then normalizing the result so that	
a. Entropy estimation for an honest server	20	$\sum_j p_j = 1$ [1, 2, 5]. Note that the sum of the independent	
b. Correction to the min-entropy	21	p_j is already $\sum_j p_j = 1 + O(1/\sqrt{D})$ before normalization.	
2. Repeated bitstrings	21	That is, for large D the normalization introduces a small	
a. Probabilities for repeated bitstrings	22	correlation between the previously independent p_j that	
b. Linear cross-entropy with unique bitstrings	23	can be typically ignored.	
c. Adversarial postselection of repetitions	24		
3. Additional statistical tests	24	Approximate sampling of a random quantum circuit	
a. Hamming distance filter	24	can be described by the probabilities	
b. Statistical test of large probabilities	25		
4. Randomness extractor	25	$p_j^F = F p_j + (1 - F) \Xi_j$	(A4)
a. Trevisan’s extractor and HMAC	26		
b. Benchmark results	26	where F corresponds to the fidelity, p_j is the ideal or	

simulated probability for the j th bitstring output of the quantum circuit, and Ξ_j is a function over bitstrings corresponding to the effect of noise. In the quantum case, ρ is the output of an experiment, $p_j^F = \langle j | \rho | j \rangle$, $F = \langle \psi | \rho | \psi \rangle$ where $|\psi\rangle$ is the ideal noiseless output, and Ξ is defined by the equation $\rho = F |\psi\rangle\langle\psi| + (1 - F)\Xi$. Note that $\sum_j \Xi_j = 1$. For simplicity we sometimes denote $\Xi_j = 1/D$, the global depolarizing channel.

In cross-entropy benchmarking (XEB) we use the expectation value of a random variable $f(p_j)$, which is defined as a function of the ideal probabilities p_j . That is, we associate the real value $f(p_j)$ to each sampled bistring $|j\rangle$. We require $f(p_j)$ to be $O(1)$ and f smooth. For linear XEB $f(p_j) = Dp_j - 1$ and for log XEB $f(p_j) = \log(Dp_j) + \text{Euler constant}$ [6]. In the following we assume that the output distribution is sufficiently close to the Porter-Thomas distribution, see Refs. [4, 6] and below.

The expectation value of $f(p_j)$ when sampling with noisy probabilities p_j^F is

$$\sum_j p_j^F f(p_j) = F \sum_j p_j f(p_j) + (1 - F) \sum_j \Xi_j f(p_j).$$

The sum in the left hand side is an expectation value estimated with RCS sampling, within an statistical error $O(1/\sqrt{k})$ where k is the size of the sample. We explain below how to obtain the value of the two sums in the right hand size analytically for large circuits. Therefore solving for F we obtain an estimator of the fidelity for any function $f(p_j)$ as specified above.

Consider first the term $p_j f(p_j)$. The expectation value over random circuits for fixed j is

$$\langle\langle p_j f(p_j) \rangle\rangle = D \int_0^\infty dp e^{-Dp} p f(p), \quad (\text{A5})$$

where $\langle\langle \cdot \rangle\rangle$ is the average over random circuits. Note that from the assumptions on f above it also follows that $\langle\langle p_j f(p_j) \rangle\rangle$ is $O(1/D)$. Furthermore, the variance over random circuits for fixed j is

$$\text{Var}(p f(p)) \in O\left(\frac{1}{D^2}\right). \quad (\text{A6})$$

We saw above that the probabilities p_j are almost independent. Treating the sum over j as a sum of independently and identically distributed (i.i.d) random variables, we have, by the central limit theorem,

$$\sum_j p_j f(p_j) = D^2 \int_0^\infty dp e^{-Dp} p f(p) + O\left(\frac{1}{\sqrt{D}}\right) \quad (\text{A7})$$

Now we consider the term $\Xi_j f(p_j)$. We assume that, when averaged over random circuits for fixed j , the random variables Ξ_j and $f(p_j)$ are independent. Therefore

$$\langle\langle \Xi_j f(p_j) \rangle\rangle = \langle\langle \Xi_j \rangle\rangle \langle\langle f(p) \rangle\rangle, \quad (\text{A8})$$

where

$$\langle\langle f(p) \rangle\rangle = D \int_0^\infty dp e^{-Dp} f(p). \quad (\text{A9})$$

We also assume that

$$\langle\langle \Xi_j \rangle\rangle \in O\left(\frac{1}{D}\right). \quad (\text{A10})$$

Therefore

$$\text{Var}(\Xi_j f(p_j)) \in O\left(\frac{1}{D^2}\right). \quad (\text{A11})$$

Treating again the sum over j as a sum of i.i.d variables we obtain

$$\sum_j \Xi_j f(p_j) = \langle\langle f(p) \rangle\rangle \sum_j \langle\langle \Xi_j \rangle\rangle + O\left(\frac{1}{\sqrt{D}}\right) \quad (\text{A12})$$

$$= \langle\langle f(p) \rangle\rangle + O\left(\frac{1}{\sqrt{D}}\right), \quad (\text{A13})$$

where we used $\sum_j \Xi_j = 1$. We conclude that the averaged effect of noise Ξ_j can be approximated as a totally depolarizing channel.

For linear XEB we have $f(p) = Dp - 1$ and therefore

$$\begin{aligned} \sum_j p_j f(p_j) &= D^2 \int_0^\infty dp e^{-Dp} p (Dp - 1) + O\left(\frac{1}{\sqrt{D}}\right) \\ &= 1 + O\left(\frac{1}{\sqrt{D}}\right) \end{aligned} \quad (\text{A14})$$

$$\begin{aligned} \sum_j \Xi_j f(p_j) &= D \int_0^\infty dp e^{-Dp} (Dp - 1) + O\left(\frac{1}{\sqrt{D}}\right) \\ &= 0 + O\left(\frac{1}{\sqrt{D}}\right). \end{aligned} \quad (\text{A15})$$

We obtain the same result for log XEB $f(p_j) = \log(Dp_j) + \text{Euler constant}$ [6]. Therefore we have

$$F \simeq \langle Dp - 1 \rangle_{\text{experiment}} \quad (\text{A16})$$

$$\simeq \langle \log(Dp_j) + \text{Euler constant} \rangle_{\text{experiment}}. \quad (\text{A17})$$

We now check numerically at what depth the output distribution becomes Porter-Thomas. Figure 1 shows that the probabilities p_j truly follow a Porter-Thomas distribution (as measured by the Kolmogorov-Smirnov test) only if the linear XEB is exponentially close to its limit value. The scaling in the x axis come from the variance (see also Ref. [6])

$$\text{Var}(\text{lin XEB}) \simeq D^2 \text{Var}(p_j^2) = \frac{2}{D}. \quad (\text{A18})$$

Nevertheless, we find numerically and experimentally that XEB serves as an estimator of fidelity before this point, and closer to the transition point in Fig. 1A of the main text, as we don't require exponential $O(1/\sqrt{D})$ precision for this estimation.

Appendix B: Device characterization and benchmarking

1. Gate Optimization

The gate fidelities of the quantum processor are carefully optimized through a series of steps. The first step

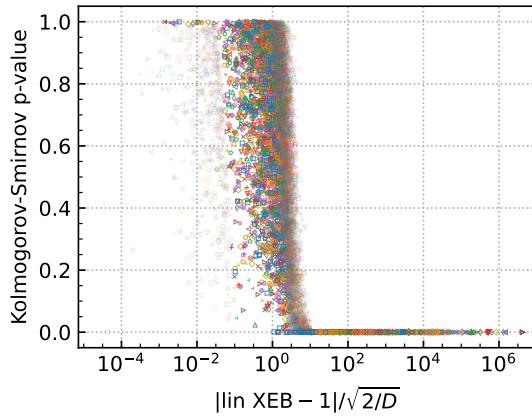


FIG. 1. The y -axis is the Kolmogorov-Smirnov p -value between the probabilities p_j at a given cycle and the Porter-Thomas distribution. The x axis is the distance of linear XEB to the ideal value in units of standard deviation. Each point corresponds to a different circuit size (with number of qubits ranging from $n = 8$ to $n = 25$) for a given fixed cycle. Lighter points correspond to datapoints outside the 90%. For all the instances, the pattern ABCDCDAB is used.

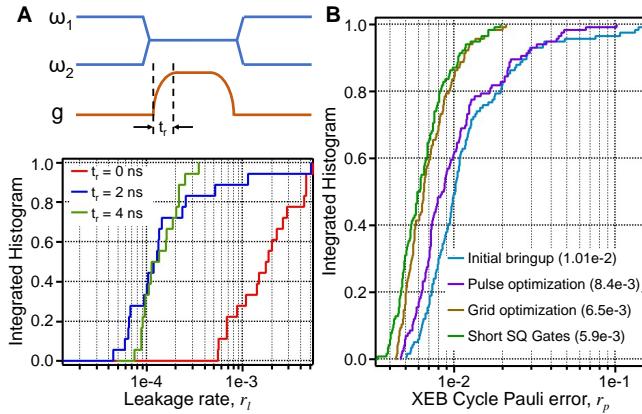


FIG. 2. Gate fidelity optimizations. (A) Upper panel: Schematic showing the flux pulses which detune the qubit frequencies (ω_1 and ω_2) and the inter-qubit coupling g during the iSWAP-like gate. A cosine filter with a rise time t_r is applied to the pulse on g . Lower panel: Integrated histograms of leakage per iSWAP-like gate, measured with three different values of t_r . Each histogram includes an identical set of 19 qubit pairs. (B) Integrated histograms of two-qubit Pauli error per cycle (which includes contributions from two single-qubit gates and one iSWAP-like gate) obtained from parallel XEB taken after different optimization steps indicated by the legend. Each histogram includes all qubit pairs on the quantum device. The median values of different histograms are quoted within the parentheses of the legend.

involves shaping of the flux pulses used to realize the iSWAP-like gates, schematically shown in Fig. 2A. Here the computational states of two qubits, $|10\rangle$ and $|01\rangle$, are brought into resonance by pulsing the qubit frequencies ω_1 and ω_2 to nearly identical values. An inter-qubit cou-

pling g is then pulsed to a maximum value of $g_{\max} \sim -13$ MHz over $t_p = 20$ ns to enable a complete population transfer from $|10\rangle$ to $|01\rangle$.

An important error channel for such a two-qubit gate is the off-resonant oscillation between the $|11\rangle$ and $|02\rangle$ (as well as $|20\rangle$) states, which may result in appreciable leakage outside the computational space at the end of the pulses. One possible strategy for mitigating leakage is through simultaneous optimization of g_{\max} and t_p such that the minima in leakage and iSWAP angle errors are synchronized [7]. However, due to the spread in qubit anharmonicities, such an optimization needs to be done for each individual qubit pair and is therefore a time-consuming process. An alternative method is to increase the rise time of the coupler pulse such that the transitions $|11\rangle \leftrightarrow |02\rangle$ and $|11\rangle \leftrightarrow |20\rangle$ are both adiabatic, thereby eliminating the need for synchronization. The leakage rates per iSWAP gate r_l , measured using a method adapted from Floquet calibration and applied to the two-excitation subspace [8], are shown in the bottom panel of Fig. 2A. We observe that for short rise times in the coupler pulse ($t_p = 0$ ns), r_l in excess of 10^{-3} is observed for most qubit pairs. The leakage rate is suppressed as t_p is increased to 2 ns, although outlier qubit pairs with $r_l > 10^{-3}$ are still observed. For $t_p = 4$ ns, all pairs tested show $r_l < 4 \times 10^{-4}$. We therefore employ $t_p = 4$ ns for experiments described in this work.

The pulse shape optimization of the iSWAP-like gates has led to a reduction in two-qubit cycle Pauli errors r_p in parallel two-qubit XEB from an initial median value of 1.01×10^{-2} to 8.4×10^{-3} , as shown in Fig. 2B. In the same plot, we show two additional optimization steps that have further improved gate fidelities: By optimizing qubit frequency placements on the 2D grid [9] to mitigate cross-talk and coupling to two-level system (TLS) defects, we reduce r_p to 6.5×10^{-3} . Finally, r_p is reduced to only 5.9×10^{-3} by shortening the execution time for the single-qubit gates from 25 ns to 18 ns.

After minimizing the cycle errors in two-qubit parallel XEB experiments, we benchmark performance of larger system sizes by performing a 4-qubit XEB experiment on ten different choices of 4 qubits across the quantum processor. We detect a substantial difference between the measured four-qubit cycle error and the predicted four-qubit cycle error based on two-qubit XEB measurements, as shown in the left panel of Fig. 3A. The average 4-qubit cycle errors are over 30% higher than predicted values. Through further characterizations, this discrepancy is understood to be arising from distortions in qubit flux pulses which lead to a slow settling of the qubit frequencies even after the pulses have nominally ended (a.k.a. “z-tails”). To mitigate the impact of z-tails, we pad the moments between the two-qubit gates and single-qubit gates in the random circuits by an idling time. The right panel of Fig. 3A shows the average difference between the measured and predicted four-qubit XEB cycle errors as a function of the padding time, where we observe that a padding time of 4 ns is sufficient to reduce

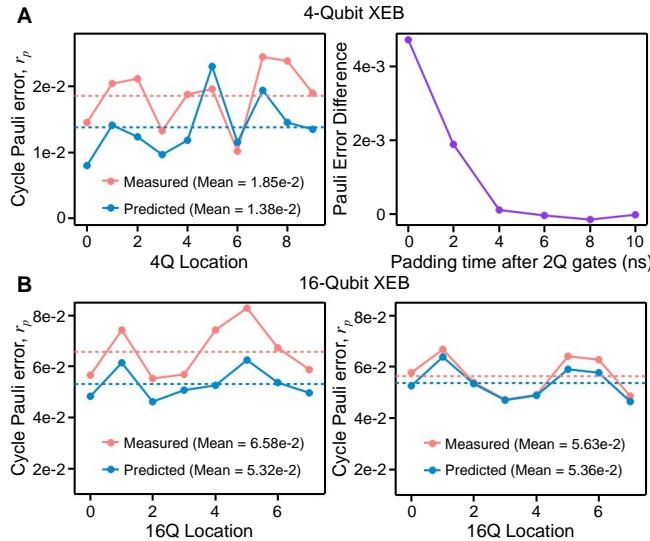


FIG. 3. Mitigating impact of z-tails. (A) Left panel: Comparison between the cycle Pauli error of a 4-qubit XEB experiment and the prediction from parallel 2-qubit XEB experiments. Horizontal axis corresponds to different 4-qubit choices. Dashed line indicates the mean values of the measured and predicted errors. Right panel: Mean difference between the measured and predicted 4Q XEB cycle errors as a function of padding times after the iSWAP-like gates. (B) Left panel: Comparison between the cycle Pauli error of a 16-qubit XEB experiment and the prediction from parallel 2-qubit XEB experiments. Horizontal axis corresponds to different 16-qubit choices. Dashed line indicates the mean values of the measured and predicted errors. Right panel: Same as the left panel but with median qubit detunings during the iSWAP-like gate reduced from 80 MHz to 40 MHz.

the difference to nearly 0. This additional padding time has been applied to experiments described in this work.

Having reached agreements between two-qubit and four-qubit XEB experiments, we compare two-qubit parallel XEB predictions with 16-qubit XEB experiments. The initial result is shown in Fig. 3B, where we again find that the measured 16-qubit XEB cycle errors are 24% higher than predictions, even with padding between single- and two-qubit gates. To reduce this discrepancy, we have re-optimized the qubit frequency placements and reduced the detunings of the qubits during the iSWAP-like gates by a factor of two. The 16-qubit parallel XEB cycle errors measured after this qubit frequency re-optimization agrees closely with the predicted values from two-qubit parallel XEB measurements.

2. Benchmarking of gates and readout

In order to construct the error model for a random circuit, we use several experiments to predict the error rate of each element. The single qubit error is calibrated through Randomized Benchmarking using only

$\pi/2$ -pulses. For the RB, we use 5 different cycles logarithmically spaced up to a thousand Clifford, with 10 random Clifford circuit instances with 600 repetition per number of cycles and circuit. The two-qubit dressed error is measured through parallel XEB after optimizing for a phased-fSim model. We used 20 random circuit instances, with 10 linearly spaced depths up to 150 cycles. The readout error is measured by preparing a random bitstring state and measuring the Probability of wrong labeling of each qubit. The error is average between the measurement error of the state $|0\rangle$ and $|1\rangle$. Finally, T_1 and T_2 Echo, used for the idling on the edges of each patches, is measure through standard population decay experiment and Echo measurement. Fig. 4F shows the improvement over the results from [6] with the dash line reporting the average fidelity achieved at the time. Every aspect of the experiment has improved, with a notable contribution from readout fidelity.

In Fig. 5, we report the angles of the iSWAP-like gate measured with parallel XEB. We note that the C-phase of the gate is now closer to $\pi/10$ compared to $\pi/6$ in [6].

Appendix C: Additional experimental data

1. Phase-matching RCS experiment

When performing a two-qubit gate, the actual unitary applied to the qubits differs from the ideal fSim by extra single-qubit Z-rotations from two sources: 1) the qubits are detuned during the gate, and 2) the qubit interaction Hamiltonian terms are not time-independent but rather oscillate due to the frequency difference between the qubits. The rotations arising from (1) do not depend on the time when the gate is applied, but the rotations arising from (2) do depend on this time, with a time-dependent phase $\gamma(t) = 2\pi(f_1 - f_0)t$.

When running quantum circuits, we typically implement Z-rotations as "virtual" gates by changing the phase of applied microwave pulses. This is equivalent to a circuit-level transformation where Z gates are pushed through the circuit by commuting them past other gates. The extra Z rotations associated with fSim gates can also be handled in this way by compiling them into the pulse sequence; in this case we say the fSim gates are "phase-matched". We can also ignore these extra Z rotations when compiling and then account for them in simulation by applying the appropriate time-dependent unitary for each gate instead of the ideal fSim unitary; in this case we say the fSim gate "non-phase-matched". Note that Z-rotations only commute through fSim when θ is 0 or $\pi/2$, that is, for cphase-like or iswap-like gates. If the gate is not exactly iswap-like, then commuting Z-rotations through it for phase-matching introduces some error, which we can see in the slightly lower XEB fidelity when using phase-matched gates.

We have also run the RCS experiment on 70 qubits using frame tracked and phased matched gate. To avoid

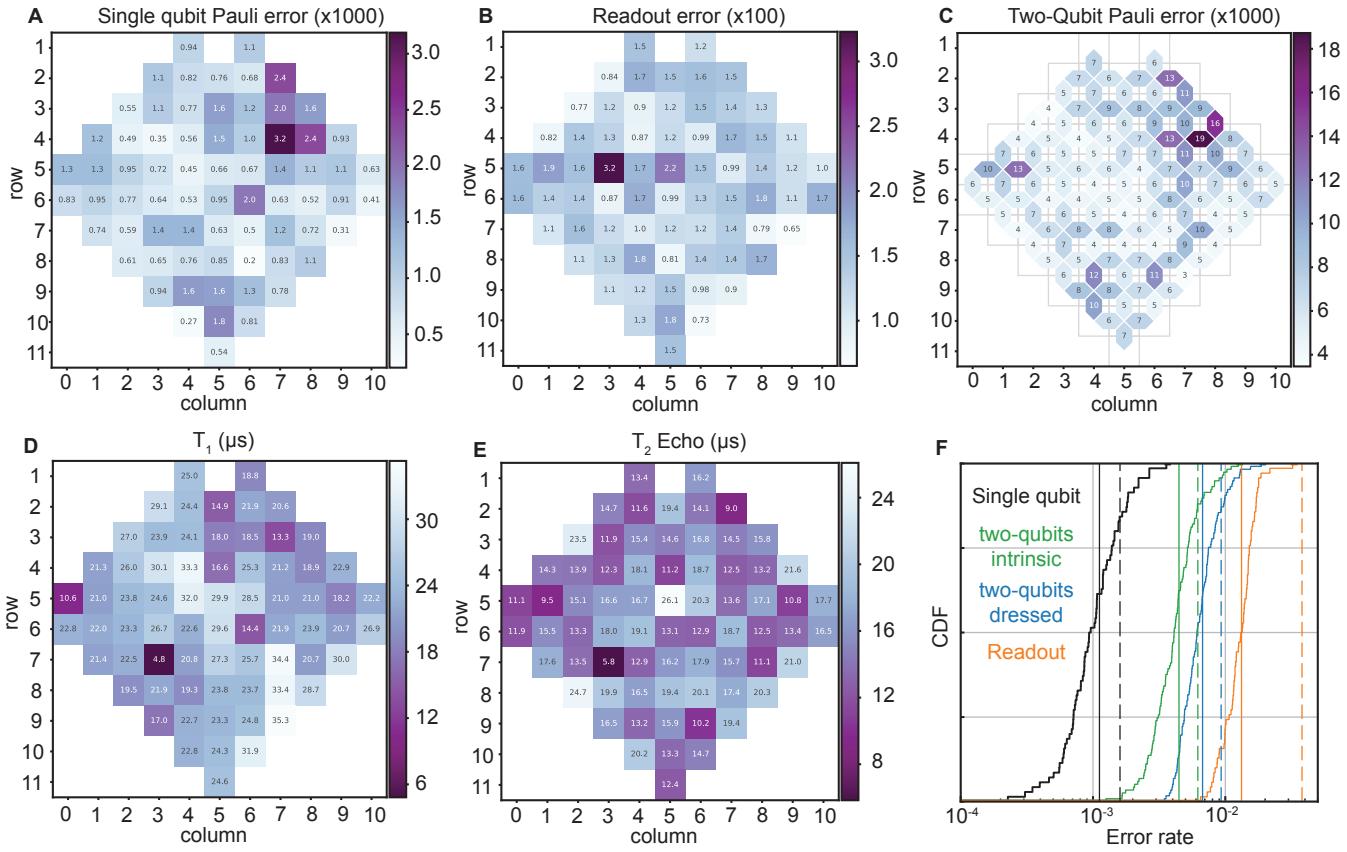


FIG. 4. **Benchmarking of the device:** Benchmarking of the random circuits elements. **A:** Single qubit Pauli Error rate measured with Randomized Benchmarking. **B:** Readout error rate measured by preparing random bitstrings and averaging the errors over the bitstrings. **C:** Two qubit Pauli Error rate measured with parallel 2-qubit XEB. **D** and **E:** T_1 and T_2 Echo times. **F** CDF of the different errors, continuous vertical line is the average, and dashed line corresponds to the average from Ref. [6].

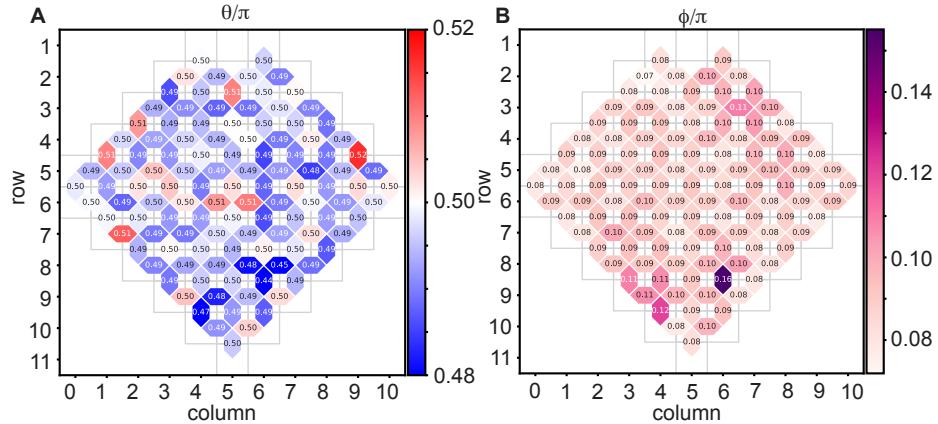


FIG. 5. **ISWAP-like characterization:** Measured angle of the iSWAP-like gate. On average, the angles are $\theta = 0.495(0.009) \times \pi$ and $\phi = 0.09(0.01) \times \pi$

adding extra physical Z-gate, we assume that all the gates have a perfect swap angle and use virtual Z gates to do both frame tracking and phase matching. The result can be seen in Fig. 6. Due to the imperfection in the calibration of the swap angle, the total fidelity of the cir-

cuits is lower than the non-phased matched, non frame tracked case presented in the main text. However, the error model correctly takes into account this discrepancy. We also present in this dataset a beyond classical exper-

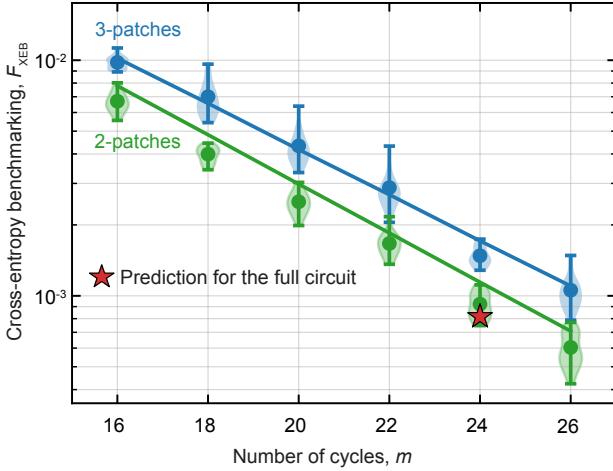


FIG. 6. **Phased matched Random Circuit Sampling experiment:** We validate our error model with 2-patches and 3-patches XEB similar to the data in main text. The red star represent the estimated fidelity of the beyond classical experiment.

iment with a fidelity predicted above 0.7×10^{-3} .

2. Adding noise

In order to probe the noise induced phase transition, we artificially increase the single qubit error rate by adding random rotations after each layer of single qubit gates in the circuit run on the hardware. The random single qubit gates are of the form:

$$U = Z^z Z^a X^x Z^{-a} \quad (\text{C1})$$

where z and x are sampled from a normal distribution center on zero and with a standard deviation given by the injected noise amplitude A . The axis a is randomly sampled from a normal distribution centered on -1 with a standard deviation of 1. In order to avoid correlated noise, the random gates are different from layer to layer in a single circuit and from circuit to circuit. These extra gates are not used in the classical simulation. Figure 7 A shows the insertion of the random single qubits gates is done on each single qubit cycle of a random circuit. In Figure 7 B we verify that adding these extra single qubit gates results in an average noise that scales as the square of the error angle, as expected.

3. Noise phase transition extended data

In this appendix, we show the full dataset used for the characterization of the Noise induce phase transitions identified in the main text. See Figs. 8 and 9.

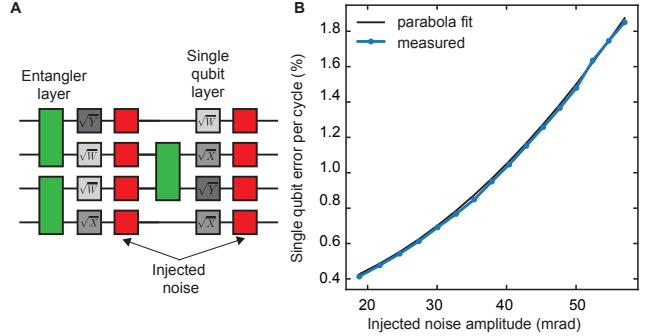


FIG. 7. **Controlling error rate.** A: Singles qubit gates with random rotations are added after each single qubit layer. B: Single qubit error rate with the added random rotations measured with single qubit XEB. The error rate follows a parabolic law.

Appendix D: Linear XEB via population dynamics

1. Population dynamics for the uniformly random single qubit gate ensemble

The linear XEB over circuits may be written as

$$\text{XEB}(t) = 2^n C - 1, \quad (\text{D1})$$

$$C = \sum_z \langle z | U \rho_0 U^\dagger | z \rangle \langle z | \mathcal{E} [U \rho_0 U^\dagger] | z \rangle, \quad (\text{D2})$$

where \mathcal{E} corresponds to a noisy evolution channel. We now explain how it's average can be calculated via population dynamics [10, 11].

Consider first a noise free evolution. Note that the average probability has the form of an out-of-time ordered correlator, $C = \sum_z \text{Tr}\{\mathcal{O}_z \rho_0(t) \mathcal{O}_z \rho_0(t)\}$ where $\mathcal{O}_z = |z\rangle\langle z|$, and $|z\rangle = \otimes_{i=1}^n |z_i\rangle$, $z_i = \{0, 1\}$ is an n qubit computational basis state. It can be described in terms of two copies of the evolution $\rho_0(t) \otimes \rho_0(t)$. After averaging over uniformly random (Haar) single qubit gates the dynamics in such doubled operator space is fully described in terms of two invariants: identity operator $\mathbb{1}$ and $\mathcal{B} = (1/3) \sum_{\alpha=x,y,z} \sigma^\alpha \otimes \sigma^\alpha$, where σ^α are Pauli operators.

The average dynamics of a pair of identical operators $\mathcal{O}(t) \otimes \mathcal{O}(t)$ in the n qubit system subject to a circuit consisting of cycles with two-qubit gates can be described by a time dependent distribution $P(\{v_i\}, t)$ over an n bit register $\{v_i\}$, $v_i \in \{0, 1\}$ corresponding to $\{\mathbb{1}_i, \mathcal{B}_i\}$, respectively. That is,

$$\overline{\mathcal{O}(t) \otimes \mathcal{O}(t)} = \sum_{\{v_i\}} P(\{v_i\}, t) \bigotimes_i ((1 - v_i) \mathbb{1}_i + \mathcal{B}_i v_i). \quad (\text{D3})$$

For operators which satisfy $\mathcal{O}^2 = 1$ (true for Pauli operators) the coefficients are normalized probabilities

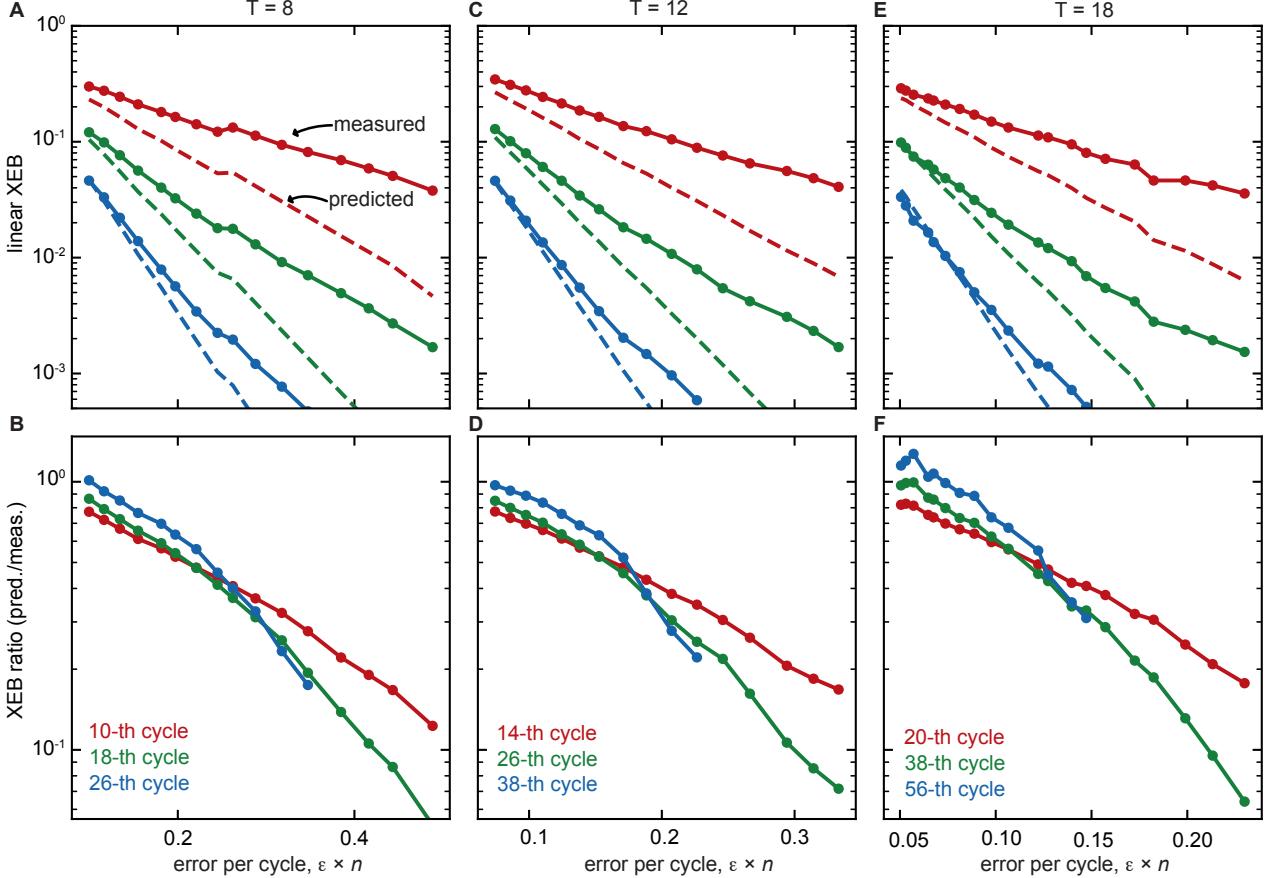


FIG. 8. **Weak-link model:** See main text Fig. 4 for more details. The first row shows the measured XEB value as a function of the error per cycle. In the strong noise regime, the measured XEB value is far from the expected value, whereas in the weak noise, and sufficient depth, the measured value is correctly predicted by the component fidelity of the circuit. The second row shows the XEB ratio.

$\sum_{\{v_i\}} P(\{v_i\}, t) = 1$. Each two-qubit gate defines a Markov process with the update matrix,

$$P(\{v_i\}, t+1) = \sum_{v'_j v'_k} \Omega_{v_j v_k, v'_j v'_k} P(\{v'_i\}, t). \quad (\text{D4})$$

where the indexes j and k correspond to the qubits involved in the corresponding two-qubit gate.

We can take the two-qubit gate to be approximately equal to an iSWAP, $U_{ij} = \exp(-i\frac{\pi}{4}(X_i X_j + Y_i Y_j))$, for which the population dynamics update corresponds to

$$\hat{\Omega}^{(i,j)} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \end{pmatrix}. \quad (\text{D5})$$

Elements of the matrix $\hat{\Omega}$ correspond to the transition probabilities between different configurations induced by the application of a two-qubit gate. $\hat{\Omega}_{10,01}$ corresponds to \mathcal{B} hoping from one qubit to another ($\Omega_{10,01} = \frac{1}{3}$ for

iSWAP) whereas $\Omega_{10,11}$ corresponds to creation of a new \mathcal{B} ($\Omega_{10,11} = \frac{2}{3}$ for iSWAP).

The contribution of each configuration to XEB is determined by individual invariants, $(\mathbb{1}_i, \mathcal{B}_i) \rightarrow (1, 1/3)$ as

$$\text{XEB} = 2^n \sum_{\{v_i\}} \frac{1}{3^{\sum v_i}} P(\{v_i\}, t) - 1. \quad (\text{D6})$$

To include the effects of noise the two-qubit gate cycle update rules need to be supplemented with the noise-induced decay rules at each two qubit cycle [10],

$$\mathbb{1}_i \mathbb{1}_j \rightarrow \mathbb{1}_i \mathbb{1}_j, \quad (\text{D7})$$

$$\mathcal{B}_i \mathbb{1}_j \rightarrow \exp(-\frac{16}{15} p_2) \mathcal{B}_i \mathbb{1}_j, \quad (\text{D8})$$

$$\mathcal{B}_i \mathcal{B}_j \rightarrow \exp(-\frac{16}{15} p_2) \mathcal{B}_i \mathcal{B}_j, \quad (\text{D9})$$

where p_2 is the two-qubit depolarizing error.

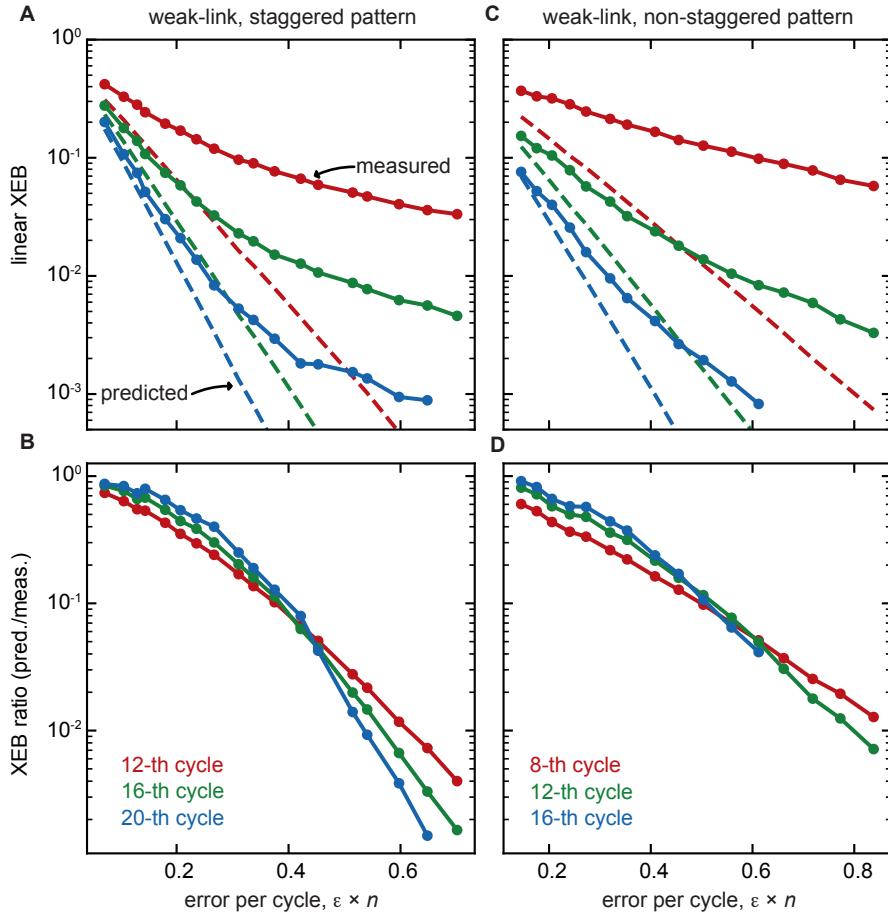


FIG. 9. Noise phase transition in 2D: The first row shows the measured XEB as a function of the error per cycle. In the strong noise regime, the measured XEB value is far from the expected value. See main text Fig. 4 for more details about the different patterns. For very strong noise, and large number of cycles the linear XEB value starts to be hard to measure and requires a large number of repetitions, making these measurements challenging.

2. Convergence of population dynamics to Porter-Thomas

The initial state for population dynamics is obtained by averaging the initial bitstring $\rho_0 = \prod_i (\mathbb{1}_i + Z_i)/2$ over the first layer of single qubit gates. The result of this averaging is $\prod_i (\mathbb{1}_i + \mathcal{B}_i)/4$. It can be interpreted as equal weight distribution $P(\{v_i\}, 0) = 1/2^n$ over all configurations $\{v_i\}$. After the first layer of one qubit gates $\text{XEB} = (4/3)^n$.

In a multi-qubit system a layer of gates corresponds to the evolution under $\hat{\Omega}^{(i,j)}$ applied to each pair of qubits subject to a gate of the layer. The circuit can be characterized by a transfer matrix $\hat{\mathcal{T}}$ that consists of a product of the layers that appears periodically, such that the whole circuit corresponds to $\hat{\mathcal{T}}^d$.

There are two steady states of this Markov chain: (i) the vacuum $\{v_i = 0\}$ for all i , (ii) the thermal state that corresponds to $P(\{v_i\}) = \prod_i p(v_i)$, where $p(0) = 1/4$ and $p(1) = 3/4$. At long times in the noise free Porter-

Thomas limit, $C = 2/(2^n + 1)$, and $\text{XEB} \approx 1$. Note that the vacuum configuration $\mathbb{1}^{\otimes n}$ does not evolve, and in the presence of noise in the long depth limit the vacuum is the only remaining configuration. This produces the only non-vanishing contribution to C , resulting in $\text{XEB}=0$.

3. Weak-link model analytical solution

In this section we provide details justifying Eq. (2) of the main text. We consider an example that can be analyzed analytically: a chain with a weak link connecting its two halves A and B , that was introduced in the main text. At the weak link a two-qubit gate is applied only at depths mT where T is the number of layers applied to the rest of the chain. We describe the dynamics of XEB using the population dynamics formalism introduced in Ref. [10].

We assume T is long enough to establish the “thermal” (or Porter-Thomas) state in each half of the chain

independently. We introduce probabilities of four possible population dynamics configurations after time T : $g_{00}, g_{01}, g_{10}, g_{11}$ corresponding to both halves in the vacuum state, one half in the vacuum state and one in the thermal state and both halves in the thermal state. Initially all four configurations g_{ij} give order one contributions to linear XEB, despite having exponentially different probability in the $\{v_i\}$ basis, due to the term $1/3^{\sum v_i}$ in Eq. D6.

A single application of the weak link gate after T cycles updates these probabilities as follows,

$$g_{00}(t+T) = g_{00}(t), \quad (\text{D10})$$

$$g_{01}(t+T) = F^{T/2} \frac{1}{4} g_{01}(t), \quad (\text{D11})$$

$$g_{10}(t+T) = F^{T/2} \frac{1}{4} g_{10}(t), \quad (\text{D12})$$

$$g_{11}(t+T) \simeq F^T g_{11}(t), \quad (\text{D13})$$

where as before F is the fidelity per layer for the whole chain excluding the weak link, and the factor $1/4$ comes from the two-qubit iSWAP gate. In the last equation we drop the contribution of g_{10} to g_{11} because it adds only an exponentially small contribution to XEB. This is because the initial thermal + vacuum state has exponentially smaller probability, as explained above. We therefore find

$$\text{XEB}(m\tau) = F^{mT} + 2 \left(\frac{1}{4} F^{T/2} \right)^m. \quad (\text{D14})$$

This gives a criteria for XEB to serve as a good fidelity estimate for the chain with weak link,

$$F^T > \frac{1}{16}. \quad (\text{D15})$$

4. Numerical analysis of the phase transitions

In this section we provide numerical simulation of XEB dynamics justifying the analysis of the data in the main text. Linear XEB is calculated numerically using the exact mapping on population dynamics introduced above, see Eq. (D6). The time dependence of weights $P(\{v_i\}, t)$ is computed by applying the transfer matrices corresponding to each two-qubit gate, Eq. (D4). This method requires memory that scales exponentially as 2^n because we evolve the full probability vector. At the same time it predicts the dynamics of the average linear XEB in the presence of noise and is quadratically more efficient than direct simulation of a noisy density matrix. Without loss of generality we simulate a simplified model of the noise including only single qubit noise applied to each qubit after each layer of two qubit gates.

We first demonstrate the finite size critical scaling near the dynamical transition. Fig. 10 is a numerical analog of Fig. 2 A of the main text, showing the depth dependence of linear XEB for a fixed error rate per qubit $\epsilon = 0.01$

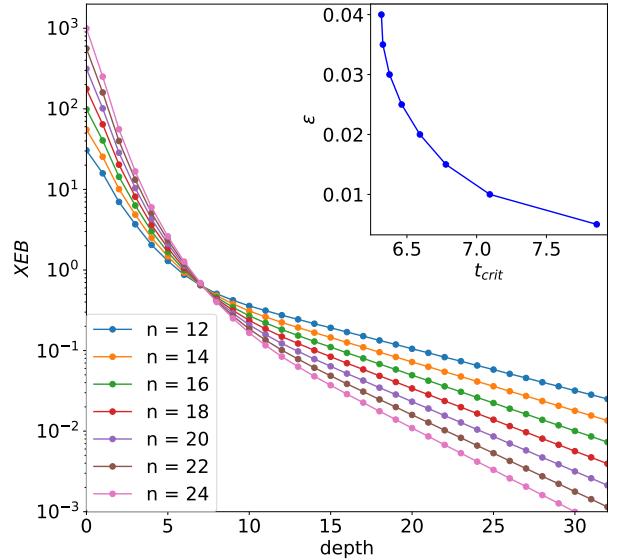


FIG. 10. XEB as a function of depth for different size n qubit chains. The error per qubit per unit time is $\epsilon = 0.01$. Inset shows the dependence of the critical depth on the error per qubit per unit time.

and different size chains. The scaling of linear XEB with the system size changes from growth to decay at the transition point, whose value is approximately size independent. This transition can be analytically continued to the anti-concentration point identified for noise free random circuits [12]. The population dynamics expression for the linear XEB, Eq. (D6) can be interpreted as a partition function of a $t \times n$ classical Ising model, where t is the depth. Discontinuity in this partition function therefore indicates a phase transition. The appropriate thermodynamic limit corresponds to scaling depth with the logarithm of the system size $t = \tau \log_2 n$. The transition point is $\tau \approx 1$ with corrections due to error per cycle $\epsilon n \sim O(n^0)$.

The noise induced phase transition (NIPT) is characterized by the change in the depth dependence of the order parameter $\Theta \equiv \exp(-\epsilon n d)/\text{XEB}$. Fig. 11 shows the depth dependence of Θ for different values of the error per cycle $0 \leq \epsilon n \leq 1.34$. At low error the order parameter converges to a constant, whereas in the presence of a sufficiently large error per cycle the order parameter converges to zero. These two regimes are separated by the phase transition where the order parameter is roughly depth independent. This transition can also be understood in terms of the partition function of the classical $t \times n$ Ising model. The thermodynamic limit corresponds to $t \rightarrow \infty$.

In the case of the weak link model introduced in the main text and in Sec. D 3, where the system is split into

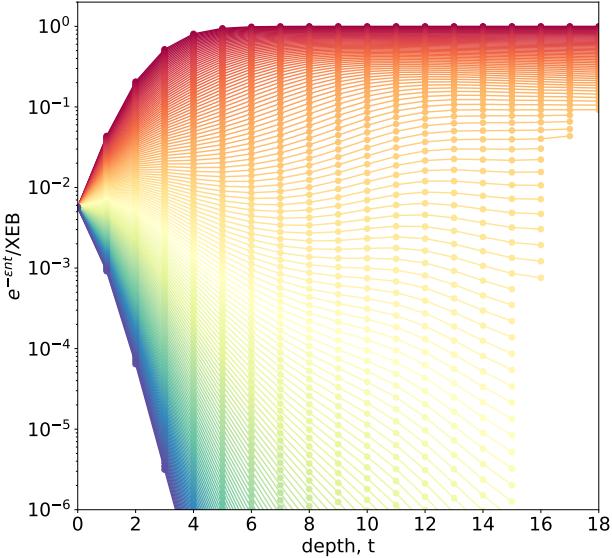


FIG. 11. Order parameter of the noise induced phase transition as a function of depth for different levels of noise for $0 \leq \epsilon n \leq 1.34$ (red to purple) on a $n = 18$ qubit chain. The link frequency is $T = 1$.

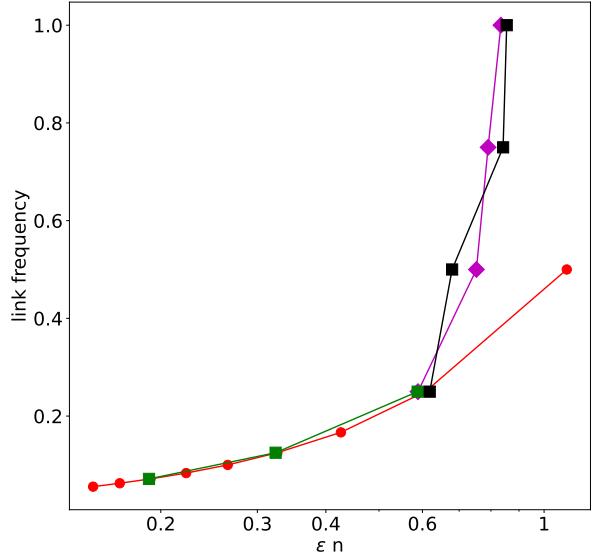


FIG. 13. Comparison of the transition point dependence on the weak link period T for the discrete gate set used in the experiment and uniformly random ensembles of single qubit gates. Black squares and magenta rhombus correspond to $n = 16$ (4×4) ABCD pattern for the experimental discrete gate set and continuous ensemble, respectively. Green squares and red circles correspond to $n = 16$ chain for the experimental and uniformly random gate set.

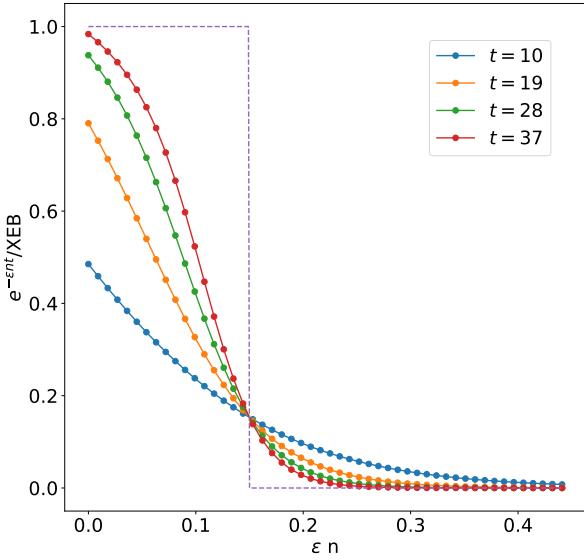


FIG. 12. Order parameter of the noise induced phase transition as a function of error per unit time for different depths on a $n = 18$ qubit chain. The link frequency is $T = 1/18$. The dashed line corresponds to the $t \rightarrow \infty$ limit.

two parts with the gates entangling the two parts applied sufficiently rarely, there is a less data intensive procedure to identify the NIPT. This relies on the crossing point of the order parameter Θ as a function of ϵn for different depths of the circuit (separated by a circuit period), shown Fig. 12. This procedure was used to identify the transition experimentally in Fig. 3 of the main text, and works well for weak link frequency $T < 1$ in 1D. In the absence of the weak link time dependence of the order parameter the method illustrated in Fig. 11 was used to identify the transition point. Numerical simulations for 2D circuits give similar results for the order parameter. The extracted transition points are summarized in the phase diagram presented in Fig. 3 G of the main text.

We compare the transition point in linear XEB for an uniformly random ensemble of single qubit gates introduced above to the discrete single qubit gate set used in the experiment. The latter maps onto population dynamics in a space of three states per qubit and is more costly to implement, requiring memory 3^n . Fig. 13 shows a comparison of the NIPT location for 16 qubit systems of two different geometries: a chain and a 4×4 system. The role of the ensemble of single qubit gates does not appear to be significant for the NIPT point.

Appendix E: Simulation of random circuit sampling using tensor network contraction

Tensor network contraction has been used extensively in the simulation of RCS over the last few years [13–20]. Given a quantum circuit, it is straightforward to generate a tensor network whose contraction yields one or many of its output amplitudes. In this tensor network, each one-qubit gate is expressed by a rank-2 tensor, each two-qubit gate is expressed by a rank-4 tensor, and the input state $|0\rangle^{\otimes n}$ is expressed by the tensor product of n rank-1 tensors.

The time and memory complexities of the contraction of such a tensor network depend strongly on the order in which tensors are contracted. Its time complexity has a lower bound related to the treewidth of the line graph of the tensor network. Ref. [21] introduced a method to alleviate the memory requirements for the contraction of a tensor network at the expense of a larger time complexity. This method involves slicing (projecting) certain carefully chosen indices in the network to the different values in their support. Each slice yields a tensor network that requires less memory to be contracted, although one has to contract a number of tensor networks that scales exponentially in the number of indices sliced. Refs. [15, 16] made substantial improvements in the optimization of contraction orderings and choice of slices.

These works focused on the contraction of an independent tensor network per output bitstring, which results in a simulation runtime that scales linearly in the number of bitstrings sampled. Specifically, an algorithm to sample from the output distribution of a quantum circuit is as follows: 1) sample bitstrings uniformly at random; 2) calculate the ideal probabilities for these bitstrings; 3) perform rejection sampling to select a subset of these bitstrings as the output. The frugal rejection sampling proposed in Ref. [22] requires computing only about 10 probabilities per output bitstring sampled. We can calculate the probabilities of $\gtrsim 10$ very similar bitstrings with just one contraction, and as we will only select one using rejection sampling and the probabilities are still uncorrelated, the result is the same as the algorithm above [23].

Ref. [19] introduced a method to compute amplitudes of a large number of uncorrelated bitstrings with a much lower overhead than linear. This implies the sparsification of the output of the tensor network as output tensors are being contracted: only those tensor entries that will lead to the computation of an amplitude of a bitstring in a pre-specified set are kept. In addition, Ref. [19] managed to make use of a special property of the fSim gate [6] in order to propagate the slicing of certain indices to other “related” indices at no extra cost. These two advancements allowed Ref. [19] to simulate sampling 1 million uncorrelated bitstrings from the largest circuit of Ref. [6] in 15 hours using 512 NVIDIA Tesla V100 SXM3 GPUs with 32GB of RAM each.

Similarly, Ref. [18] introduced dynamic programming techniques to reuse certain computations across the dif-

ferent instances of the slices taken over a tensor network. This allowed them to simulate the largest circuit of Ref. [6] in 14.5 days using 32 NVIDIA Tesla V100 GPUs with 16GB of RAM each.

In the present work we incorporate all of these advancements into a highly efficient simulated annealing optimizer in order to further reduce the time estimates for the simulation of RCS experiments. Tensor network contraction orderings, choice of sliced indices, sparsification of the output of the circuit, and reuse of intermediate computation across slicing instances, are all taken into account simultaneously in the optimization. This allows us to reduce the number of FLOPs required for the noisy simulated sampling of 1 million bitstrings from the hardest circuit of Ref. [6] by about an order of magnitude compared to the requirements of Refs. [19] and [18] when using a similar cluster with similar GPUs. When running on a Google Cloud CPU with 12 TB of memory, we estimate FLOP counts about two orders of magnitude lower than in Refs. [19] and [18]. We estimate a runtime of 2 days using a single CPU with a 20% FLOP efficiency, similar to the efficiency found in Refs. [15, 16, 19]. Table I of the main text shows the runtime estimates for the simulation of the experiments of Refs. [6, 24, 25] and the present work when run on the Frontier supercomputer.

Appendix F: Bounds to approximate tensor representations

The most promising numerical methods for more efficient approximations to random circuit sampling are based on approximate tensor representations [15, 26, 27]. Let’s write the state on n qubits as

$$|\psi\rangle = \sum_{j_1, j_2, \dots, j_n} \psi_{j_1, j_2, \dots, j_n} |j_1, j_2, \dots, j_n\rangle. \quad (\text{F1})$$

We study the simplest but illustrative case where the state is approximated with two tensors $M^{(1)}$ and $M^{(2)}$ as [27]

$$\tilde{\psi}_{j_1, j_2, \dots, j_n} = \sum_{\alpha=1}^{\chi} M_{j_1, j_2, \dots, j_l, \alpha}^{(1)} M_{\alpha, j_{l+1}, j_{l+2}, \dots, j_n}^{(2)}. \quad (\text{F2})$$

The index α is called a virtual index and χ is called the bond dimension. The state is broken into qubits on the left $[1 \dots l]$ and the right $[l+1 \dots n]$, with the virtual index encoding the entanglement between these spaces. The size of the two sub-Hilbert spaces are respectively $D_1 = 2^l$ and $D_2 = 2^{n-l}$.

Given a quantum state $|\psi\rangle$ and bond dimension χ , the best approximation of the form (F2) can be found keeping the largest χ singular values (Schmidt coefficients) of a matrix with entries corresponding to the amplitudes of $|\psi\rangle$, and row and column dimensions corresponding to

the left and right spaces. This gives the approximation

$$|\tilde{\psi}\rangle = \frac{1}{\sqrt{\sum_{\alpha=1}^{\chi} S_{\alpha}^2}} \sum_{\alpha=1}^{\chi} S_{\alpha} |l_{\alpha}\rangle |r_{\alpha}\rangle, \quad (\text{F3})$$

based on the Schmidt decomposition, where the Schmidt coefficients S are ordered from large to small. This representation is exact if the bond dimension is larger than the Schmidt rank.

For approximate matrix-product state (MPS) simulations [26, 27], the initial state is a product state with Schmidt rank equal zero. Gates involving only qubits on the left (or right) merely modify the tensor $M^{(1)}$ (or $M^{(2)}$) without affecting the Schmidt rank. However, multi-qubit gates applied on qubits belonging to both left and right partition, generally increase the Schmidt rank. The truncation of the quantum state to a fixed bond dimension $\chi \ll 2^{\min(l, n-l)}$ eventually reduces the fidelity to $F = |\langle \psi | \tilde{\psi} \rangle|^2 = \sum_{\alpha=1}^{\chi} S_{\alpha}^2$. In the next paragraphs, we quantify the fidelity for random Haar states, and we provide both numerical and analytical bounds for arbitrary states.

1. Fidelity for Haar random states

The output state of a sufficiently deep quantum random circuit can often be approximated as a Haar random state. Therefore, we can explain the fidelity obtained with representation (F2) using the distribution of singular values of a complex matrix with Gaussian entries [3] and dimension $D_1 \times D_2$, where D_1 (D_2) is the dimension of the left (right) Hilbert space. We extend the study of Ref. [27] to the case $D_1 \neq D_2$, and we assume without loss of generality $D_1 \leq D_2$.

Let S denote singular values and $s = \sqrt{D_1}S$ denote normalized singular values. The distribution of the normalized singular values follows the Marčenko–Pastur distribution [28]

$$p_{\lambda}(s) = \frac{1}{\pi} \frac{\sqrt{(\lambda_+^2 - s^2)(s^2 - \lambda_-^2)}}{\lambda s}, \quad (\text{F4})$$

with $D_1 \leq D_2$, $\lambda = D_1/D_2$, $\lambda_{\pm} = (1 \pm \sqrt{\lambda})$ and $s \in [\lambda_-, \lambda_+]$. For $\lambda = 1$, $p_{\lambda}(s)$ reduces to:

$$p(s) = \frac{1}{\pi} \sqrt{4 - s^2}. \quad (\text{F5})$$

For a given bond dimension χ the fraction of singular values is $r = \chi/D_1$. Let us define the cumulative distribution of singular values

$$C_{\lambda}(s') = \int_{s'}^{\lambda_+} ds p_{\lambda}(s) \quad (\text{F6})$$

Note that $r = C_{\lambda}(s')$ is the fraction of singular values up to a given normalized singular value s' , starting from

the largest singular values. Therefore, the normalized singular value corresponding to a given fraction r is:

$$s_{\lambda}(r) = C_{\lambda}^{-1}(r). \quad (\text{F7})$$

For $\lambda = 1$ one obtains [27]

$$s_{\lambda=1}(r) = 2 \cos \left(\frac{1}{2} \mathcal{A}^{-1}(\pi r) \right), \quad (\text{F8})$$

where $\mathcal{A}(\theta) = \theta - \sin \theta$.

The fidelity for a given fraction r of singular values is given by

$$\mathcal{F}_{\lambda}(r) = \int_{s(r)}^{\lambda_+} ds s^2 p_{\lambda}(s). \quad (\text{F9})$$

Recalling that

$$\frac{ds_{\lambda}(r)}{dr} = \frac{dC_{\lambda}^{-1}(r)}{dr} = \frac{1}{\frac{dC_{\lambda}}{ds}|_{s=s_{\lambda}(r)}} = -\frac{1}{p_{\lambda}(s_{\lambda}(r))},$$

one also gets an alternative expression

$$\begin{aligned} \mathcal{F}_{\lambda}(r') &= - \int_{r'}^0 dr \frac{1}{p_{\lambda}(s_{\lambda}(r))} s_{\lambda}^2(r) p_{\lambda}(s_{\lambda}(r)) \\ &= \int_0^{r'} dr s_{\lambda}^2(r). \end{aligned} \quad (\text{F10})$$

For $\chi \ll D_1$ we have

$$\mathcal{F}_{\lambda}(\chi/D_1) \leq \left. \frac{d\mathcal{F}_{\lambda}(r)}{dr} \right|_{r=0} \frac{\chi}{D_1} = \lambda_+^2 \frac{\chi}{D_1}, \quad (\text{F11})$$

where we used the fact that \mathcal{F}_{λ} is a monotonically increasing and strictly concave function (that is, $d^2\mathcal{F}_{\lambda}/dr^2 = -2s_{\lambda}(r)/p_{\lambda}(s_{\lambda}(r)) \leq 0$). For $\lambda = 1$ [27], the bound reduces to $\mathcal{F}_{\lambda=1} \leq \frac{4\chi}{\sqrt{D}}$. This gives an upper bound for the fidelity of a single projection into the ansatz of Eq. (F2) once the ideal state is sufficiently entangled.

2. Fidelity bound for arbitrary states

The fidelity of a Schmidt-decomposed state as in Eq. (F3) is

$$F = \sum_{\alpha=1}^{\chi} S_{\alpha}^2. \quad (\text{F12})$$

Using the Jensen's inequality, it follows that

$$\chi^2 \left(\frac{1}{\chi} \sum_{\alpha=1}^{\chi} S_{\alpha}^2 \right)^2 \leq \chi \sum_{\alpha=1}^{\chi} S_{\alpha}^4 \quad (\text{F13})$$

and therefore

$$F \leq \sqrt{\chi \sum_{\alpha=1}^{\chi} S_{\alpha}^4} \leq \sqrt{\chi \operatorname{tr} \rho_L^2}, \quad (\text{F14})$$

with $\operatorname{tr} \rho_L^2 = \sum_{\alpha=1}^{D_1} S_{\alpha}^4$ being the reduced purity after tracing out the qubits on the right. Using exact numerics for small systems (see Fig. 14), one can find a tighter bound

$$F \lesssim \mathcal{F}_{\lambda}(\chi \operatorname{tr} \rho_L^2) \leq \lambda_+^2 \chi \operatorname{tr} \rho_L^2, \quad (\text{F15})$$

with \mathcal{F}_{λ} being the fidelity for Haar random states (see Eq. F10), and the average is at fixed depth. Equations (F14) and (F15) gives an upper bound for the fidelity of a single projection for an arbitrary quantum state in the form (F2).

We can compare the numerical bound Eq. (F15) with the fidelity for Haar random states Eq. (F11) for $D_1 = \sqrt{D}$. The average purity for a Haar random state when $D_1 = \sqrt{D}$ is:

$$\begin{aligned} \langle\langle \operatorname{tr} \rho_L^2 \rangle\rangle &= \sum_{\alpha=1}^{D_1} \langle\langle S_{\alpha}^4 \rangle\rangle = \frac{1}{D_1^2} \sum_{\alpha=1}^{D_1} \langle\langle s_{\alpha}^4 \rangle\rangle \\ &= \frac{1}{D_1} \int_0^2 s^4 \frac{1}{\pi} \sqrt{4-s^2} ds = \frac{2}{\sqrt{D}}. \end{aligned} \quad (\text{F16})$$

Therefore, for small χ/\sqrt{D} , the numerical bound Eq. (F15) is only twice larger than the correct fidelity in this case.

3. Open and close simulations using approximate tensor representations

As described in [27], approximated tensor representations can be used to sample bitstrings with a given target fidelity F . More precisely, authors of [27] present two different protocols: “open” and “close” simulations.

For open simulations at fixed bond dimension χ , the circuit C is split in k sub-circuits such that $C = C_k \cdots C_1 C_0$. Starting from the initial state $|\psi_0\rangle = |0\rangle$, a new approximate state $|\tilde{\psi}_1\rangle$ is obtained by truncating the state $|\psi_1\rangle = C_1 |\psi_0\rangle$ using its χ largest singular values $\{S_{\alpha,1}\}$ only. The approximate state $|\tilde{\psi}_1\rangle$ is then evolved to get $|\psi_2\rangle = C_2 |\tilde{\psi}_1\rangle$, which is again truncated to its largest χ singular values to obtain the approximate state $|\tilde{\psi}_2\rangle$. Calling $f_k = |\langle\psi_k| \tilde{\psi}_k\rangle|^2 = \sum_{\alpha=1}^{\chi} S_{\alpha,k}^2$ the partial fidelity of the approximate state $|\tilde{\psi}_k\rangle$, Ref. [27] shows that, for random circuits, the final fidelity can be expressed as the product of all the partial fidelity, that is $F = |\langle\tilde{\psi}_k| C |\psi_0\rangle|^2 = f_1 f_2 \cdots f_k$.

For a large number of qubits, computing $|\psi_i\rangle = C_i |\psi_{i-1}\rangle$ and finding its singular values to get the approximate state $|\tilde{\psi}_i\rangle$ is numerically intractable. To overcome this limitation, authors of [27] introduce a variational approach to compute $|\tilde{\psi}_i\rangle$ without the need of the

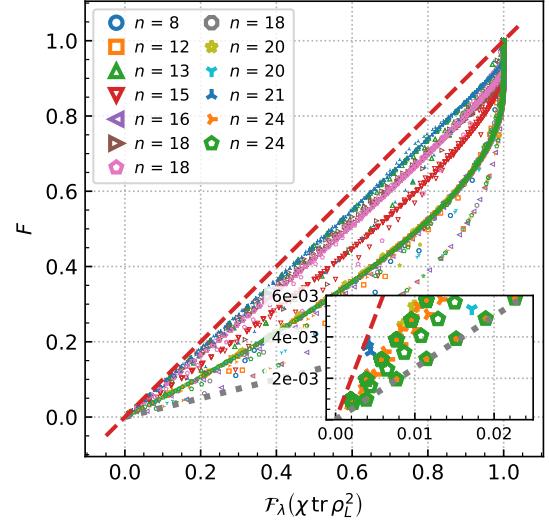


FIG. 14. Numerical fidelity bound. The plot compares the exact fidelity F for different Sycamore layouts of different sizes, cycles, and bond dimensions χ to the numerical upper-bound $\mathcal{F}_{\lambda}(\chi \operatorname{tr} \rho_L^2)$, with \mathcal{F}_{λ} and $\operatorname{tr} \rho_L^2$ being respectively the fidelity in the Haar limit and the reduced purity. The dotted-gray line corresponds to the bound $\mathcal{F}_{\lambda}(\chi \operatorname{tr} \rho_L^2) \leq \lambda_+^2 \chi \operatorname{tr} \rho_L^2 \leq 4 \chi \operatorname{tr} \rho_L^2$. For all the instances, the pattern ABCDCDAB is used, and the qubits are partitioned in two equal halves using a diagonal cut.

intermediate state $C_i |\tilde{\psi}_{i-1}\rangle$ and without explicitly computing its singular values. More precisely, for any C_i , a new random approximate tensor $|\tilde{\phi}_i\rangle$ of bond dimension χ is used to compute the objective:

$$f_i(|\tilde{\phi}_i\rangle) = |\langle\tilde{\psi}_{i-1}|C|\tilde{\phi}_i\rangle|^2. \quad (\text{F17})$$

Recalling that both $|\tilde{\psi}_{i-1}\rangle$ and $|\tilde{\phi}_i\rangle$ are MPS of bond dimension χ , computing f_i for sufficiently shallow C_i and small χ is doable even for a large number of qubits [27]. Using the update strategy proposed in [27], one can find $|\tilde{\psi}_i\rangle$ as

$$|\tilde{\psi}_i\rangle = \underset{|\tilde{\phi}_i\rangle}{\operatorname{argmax}} \tilde{f}_i(|\tilde{\phi}_i\rangle). \quad (\text{F18})$$

Because the quantum system becomes more and more entangled by applying the sub-circuits C_i , one expects that $f_{i+1} \leq f_i$, reaching the saturation value of $\mathcal{F}_{\lambda}(\chi/D_1)$ when the quantum state reaches the random Haar limit.

Close simulations at fixed bond dimension χ are useful to sample bitstrings with an improved target fidelity than the corresponding open simulations with the same bond dimension. To start, the circuit is split in three parts $C = C_2 C_M C_1$. Using the open simulation protocol, the approximate state $|\tilde{\Psi}_1\rangle$ is computed by using $|0\rangle$ as initial state and C_1 as circuit. Similarly, the approximate state $|\tilde{\Psi}_2(x)\rangle$ is computed by using the open simulation protocol with $|x\rangle$ as initial circuit and C_2^\dagger as circuit. Finally,

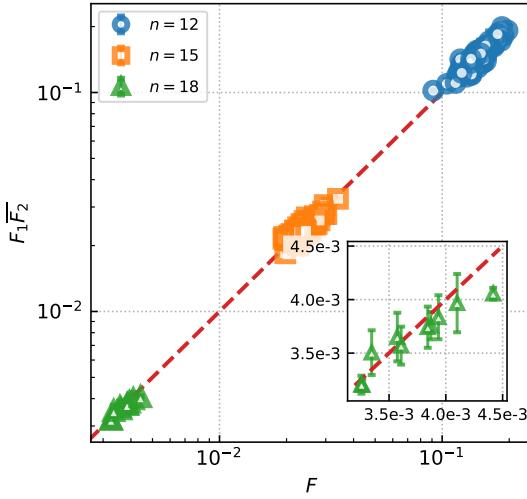


FIG. 15. Fidelity for close simulations $F_1\bar{F}_2$ (see App. F 3), compared to the exact fidelity F . The bond dimension is fixed to $\chi = 8$. Each point correspond to a different circuit, with the average being performed over bitstrings. Circuits are split in three parts of $|C_1| = 8$, $|C_M| = 4$ and $|C_2| = 8$ cycles respectively. For all the instances, the pattern ABCDCDAB is used, and the qubits are partitioned in two equal halves using a diagonal cut.

the approximate amplitude \tilde{a}_x is computed as:

$$\tilde{a}_x = \langle \Psi_2(x) | C_M | \Psi_1 \rangle. \quad (\text{F19})$$

As discussed in [27], \tilde{a}_x can be seen as amplitudes extracted from a quantum state with a fidelity $F = F_1\bar{F}_2$, with F_1 and \bar{F}_2 being the fidelity of $|\tilde{\Psi}_1\rangle$ and the average fidelity of $|\tilde{\Psi}_2(x)\rangle$ respectively. Because both $|0\rangle$ and $|x\rangle$ are MPS with bond dimension 0, $F_1\bar{F}_2$ might be larger than the fidelity one obtains with the open simulation protocol. However, unlike the open simulation, multiple runs are needed to get the required number of bitstrings.

Fig. 15 shows the fidelity of amplitudes sampled using the close simulation protocol at fixed bond dimension $\chi = 8$, compared to the exact fidelity. Each point correspond to a different circuit, and circuits are split so that C_1 and C_2 contain 8 cycles while C_M contains 4 cycles. The average is performed over bitstrings.

4. XEB for approximate tensor representations

We now explain why, at sufficiently large depth, XEB is still a good estimator of fidelity for approximate tensor representations. The optimal approximate tensor representation Eq. (F3) is based on the Schmidt decomposition, that is

$$|\tilde{\psi}\rangle = \frac{1}{\sqrt{F}} \sum_{\alpha=1}^{\chi} S_{\alpha} |\nu_{\alpha}\rangle, \quad (\text{F20})$$

where $|\nu_{\alpha}\rangle = |l_{\alpha}\rangle |r_{\alpha}\rangle$ and $F = \sum_{\alpha=1}^{\chi} S_{\alpha}^2$ is the fidelity.

We first show that in the limit of large depth the left and right singular vectors $\{|l_{\alpha}\rangle\}$ and $\{|r_{\alpha}\rangle\}$ are Haar random states. Note that these are the singular vectors of a matrix M with Gaussian entries (a Haar random matrix), see App. F 1. For any unitaries U and V we also have that UMV^{\dagger} is a matrix with Gaussian entries. This implies that the distribution of singular vectors is invariant under unitary transformation, that is, the singular vectors are Haar random. Therefore, we approximate the singular vectors as having i.i.d Gaussian random real and imaginary parts.

We first give an explanation for why XEB is a good estimator of fidelity in this case, followed by a formal proof. We can write

$$|\psi\rangle = \sqrt{F} |\tilde{\psi}\rangle + \sqrt{1-F} |\perp\rangle \quad (\text{F21})$$

where

$$|\perp\rangle = \frac{1}{\sqrt{1-F}} \sum_{\alpha=\chi+1}^{D_1} S_{\alpha} |\nu_{\alpha}\rangle. \quad (\text{F22})$$

In the case of linear XEB, $f(p_j) = Dp_j$, we have

$$\begin{aligned} D \sum_j \tilde{p}_j p_j &= F \sum_j D \tilde{p}_j^2 + (1-F) D \sum_j \tilde{p}_j \perp_j \\ &\quad + \sqrt{F(1-F)} D \sum_j 2\text{Re}(\langle j|\tilde{\psi}\rangle \langle \perp|j\rangle), \end{aligned} \quad (\text{F23})$$

where p_j are the ideal probabilities $p_j = |\langle j|\psi\rangle|^2$ and $\tilde{p}_j = |\langle j|\tilde{\psi}\rangle|^2$. For $D_1 \gg \chi \gg 1$ both $|\psi\rangle$ and $|\perp\rangle$ converge to independent Haar random states. Therefore

$$D \sum_j \tilde{p}_j^2 \simeq 2 \quad (\text{F24})$$

$$\begin{aligned} D \sum_j \tilde{p}_j \perp_j &\simeq D^2 \langle \langle \tilde{p}_j \perp_j \rangle \rangle \\ &\simeq D^2 \langle \langle \tilde{p}_j \rangle \rangle \langle \langle \perp_j \rangle \rangle \simeq 1 \end{aligned} \quad (\text{F25})$$

$$2D \sum_j \text{Re}(\langle j|\tilde{\psi}\rangle \langle \perp|j\rangle) \simeq 0, \quad (\text{F26})$$

where $\langle \langle \cdot \rangle \rangle$ denotes average over random states $|\psi\rangle$ (or circuits, see App. A). Therefore

$$D \sum_j \tilde{p}_j p_j \simeq F, \quad (\text{F27})$$

as we wanted.

We note that for very small χ , such as $\chi = 1$, linear XEB overestimates the fidelity. Indeed, in this case we have

$$D \sum_j \tilde{p}_j^2 = D \sum_{a,b} |\langle a|l_{\alpha}\rangle|^4 |\langle b|r_{\alpha}\rangle|^4 \simeq 4. \quad (\text{F28})$$

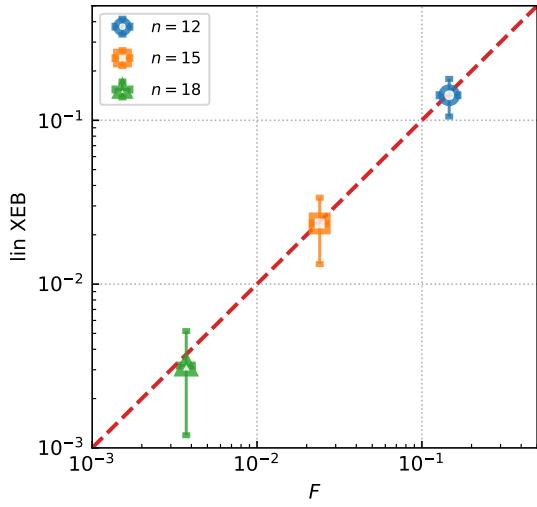


FIG. 16. The plot compares the exact fidelity F to the linear XEB for close simulations with a fixed bond dimension of $\chi = 8$. Circuits for the close simulations are split in three parts of $|C_1| = 8$, $|C_M| = 4$ and $|C_2| = 8$ cycles respectively. The error is obtained by averaging over multiple circuits. For all the instances, the pattern ABCDCDAB is used.

Nevertheless, this case is uninteresting for simulations, as $F \simeq \lambda_+^2/D_1$ corresponds to a very small fidelity. Numerical results for small quantum systems, Fig. 16, confirm the correspondence between exact fidelity and the XEB for approximate quantum states using close simulations.

We now give a detailed proof. Below till the end of this subsection, for the simplicity of notation, we will use $\mathbb{E}[\cdot]$ to denote the average over states $\langle\langle\cdot\rangle\rangle$.

We recall that for a $L \times L$ random β -Haar distributed unitary Q ($\beta = 1$ for real and $\beta = 2$ for complex and $\beta = 4$ for quaternion unitaries) with entries $q_{i,j}$ we have the following expectations (see Table IV in [29]):

expectation values
$\mathbb{E}[q_{i,j} ^4] = \frac{\beta+2}{L(\beta L+2)}$
$\mathbb{E}[q_{i,j} q_{i,k} ^2] = \frac{\beta}{L(\beta L+2)}$

We remind the reader that the exact and approximation outputs (from Eqs. (F3) and (F20)) are

$$|\psi\rangle := \sum_{\alpha=1}^{\sqrt{D}} S_\alpha |l_\alpha\rangle \otimes |r_\alpha\rangle := \sum_{\alpha=1}^{\sqrt{D}} S_\alpha |\nu_\alpha\rangle$$

$$|\tilde{\psi}\rangle := \frac{1}{\sqrt{F}} \sum_{\alpha=1}^{\chi} S_\alpha |l_\alpha\rangle \otimes |r_\alpha\rangle := \frac{1}{\sqrt{F}} \sum_{\alpha=1}^{\chi} S_\alpha |\nu_\alpha\rangle.$$

Let $p_j := |\langle j|\psi\rangle|^2$ and $\tilde{p}_j := |\langle j|\tilde{\psi}\rangle|^2$. We have $\langle j|\psi\rangle =$

$$\sum_{\alpha=1}^{\sqrt{D}} S_\alpha \langle j|\nu_\alpha\rangle$$

$$p_j = \left| \sum_{\alpha=1}^{\sqrt{D}} S_\alpha \langle j|\nu_\alpha\rangle \right|^2 = \sum_{\alpha,\beta=1}^{\sqrt{D}} S_\alpha S_\beta \langle j|\nu_\alpha\rangle \langle \nu_\beta|j\rangle,$$

$$\tilde{p}_j = \frac{1}{F} \left| \sum_{\alpha=1}^{\chi} S_\alpha \langle j|\nu_\alpha\rangle \right|^2 = \frac{1}{F} \sum_{\alpha,\beta=1}^{\chi} S_\alpha S_\beta \langle j|\nu_\alpha\rangle \langle \nu_\beta|j\rangle.$$

As stated above $\langle j|\nu_\alpha\rangle = \langle j|(|l_\alpha\rangle \otimes |r_\alpha\rangle) = v_\alpha w_\alpha$ is simply a product of two complex numbers, where v_α and w_α represent an entry of $|l_\alpha\rangle$ and $|r_\alpha\rangle$ respectively.

Lemma 1. $D\mathbb{E} \left[\sum_j p_j \tilde{p}_j \right] - 1 \approx F + O(1/\sqrt{D})$, where the expectation is over the random haar vectors $|l_\alpha\rangle$ and $|r_\alpha\rangle$ and singular values S_α .

Proof. We first compute $\mathbb{E}[p_j \tilde{p}_j]$. Treating singular values as independent from the vectors we have

$$\mathbb{E}[p_j \tilde{p}_j] = \frac{1}{F} \sum_{\alpha,\beta=1}^{\sqrt{D}} \sum_{c,d=1}^{\chi} \{ \mathbb{E}[S_\alpha S_\beta S_c S_d] \times \mathbb{E}[\langle j|\nu_\alpha\rangle \langle \nu_\beta|j\rangle \langle j|\nu_c\rangle \langle \nu_d|j\rangle] \} \times \frac{1}{F} \sum_{\alpha,\beta=1}^{\sqrt{D}} \sum_{c,d=1}^{\chi} \mathbb{E}\{ [S_\alpha S_\beta S_c S_d] \times \mathbb{E}[v_\alpha w_\alpha \bar{v}_\beta w_\beta v_c w_c \bar{v}_d w_d] \}. \quad (\text{F29})$$

First of all the vectors $|l_\alpha\rangle$ and $|r_\alpha\rangle$ are independent and power of their entries vanish over the complex field because of the invariance of Haar measure. Let

$$g_{j,\chi,D} := \frac{1}{F} \sum_{\alpha,\beta=1}^{\sqrt{D}} \sum_{c,d=1}^{\chi} \{ \mathbb{E}[S_\alpha S_\beta S_c S_d] \mathbb{E}[v_\alpha v_c \bar{v}_\beta \bar{v}_d] \times \mathbb{E}[w_\alpha w_c \bar{w}_\beta \bar{w}_d] \}. \quad (\text{F30})$$

The non-zero contributions in the sum are three cases:

- case 1: $\alpha = \beta \neq c = d$
- case 2: $\alpha = d \neq c = \beta$
- case 3: $\alpha = d = c = \beta$

Before we indulge in computing these cases one by one, let us focus on the expectation with respect to the *entries* as the entries of a Haar unitary have correlations. When $\alpha = \beta \neq c = d$ and v_α and v_c do not belong to the same row of the unitary matrix induced by singular value decomposition whose columns are $|l_\alpha\rangle$, we have

$$\mathbb{E}[|v_\alpha^{(1)}|^2 |v_c^{(2)}|^2] = \frac{1}{D} \sqrt{D} (\sqrt{D} - 1) \frac{1}{D} = \frac{1}{D} (1 - \frac{1}{\sqrt{D}}).$$

However, when $\alpha = \beta \neq c = d$ and v_α and v_c come from the *same* row or column of the unitary matrix, then from the second row of the Table above we have

$$\mathbb{E}[|v_\alpha^{(1)}|^2 |v_c^{(1)}|^2] = \frac{1}{D} \sqrt{D} \frac{\beta}{\sqrt{D} (\beta \sqrt{D} + 1)}$$

$$= \frac{1}{D} \frac{\beta}{(\beta \sqrt{D} + 1)}$$

$$= \frac{1}{D \sqrt{D}} \left(1 - \frac{1}{\beta \sqrt{D}} \right). \quad (\text{F31})$$

The latter is of lower order. We ignore the terms of lower order below and proceed to calculate the three cases by assuming that the entries do not come from the same row or column of the inducing random haar unitary matrix.

Recall from the asymptotic scaling of the purity Eq. (F16) that $\sum_{c=1}^{\chi} \mathbb{E}[S_c^4] \leq 2/\sqrt{D}$.

Case 1: $\alpha = \beta \neq c = d$. We have up to $O(1/\sqrt{D})$ from Eq. (F30)

$$\begin{aligned} g_{j,\chi,D} &= \frac{1}{F} \sum_{\alpha=1, \alpha \neq c}^{\sqrt{D}} \sum_{c=1}^{\chi} \mathbb{E}[S_{\alpha}^2 S_c^2] \mathbb{E}[|v_{\alpha}|^2 |v_c|^2] \mathbb{E}[|w_{\alpha}|^2 |w_c|^2] \\ &= \frac{1}{FD^2} \sum_{\alpha=1, \alpha \neq c}^{\sqrt{D}} \sum_{c=1}^{\chi} \mathbb{E}[S_{\alpha}^2 S_c^2] \\ &= \frac{1}{FD^2} \left(\sum_{\alpha=1}^{\sqrt{D}} \sum_{c=1}^{\chi} \mathbb{E}[S_{\alpha}^2 S_c^2] - \sum_{c=1}^{\chi} \mathbb{E}[S_c^4] \right) \\ &= \frac{1}{FD^2} \left(F \sum_{\alpha=1}^{\sqrt{D}} \mathbb{E}[S_{\alpha}^2] - \sum_{c=1}^{\chi} \mathbb{E}[S_c^4] \right) \\ &= \frac{1}{FD^2} \left(F \sum_{\alpha=1}^{\sqrt{D}} \mathbb{E}[S_{\alpha}^2] - O(1/\sqrt{D}) \right) \\ &= \frac{1}{D^2} \left(1 - O(1/\sqrt{D}) \right). \end{aligned} \quad (\text{F32})$$

Case 2: $\alpha = d \neq c = \beta$. We have up to $O(1/\sqrt{D})$ from Eq. (F30)

$$\begin{aligned} g_{j,\chi,D} &= \frac{1}{F} \sum_{\alpha=1, \alpha \neq c}^{\chi} \sum_{c=1}^{\chi} \mathbb{E}[S_{\alpha}^2 S_c^2] \mathbb{E}[|v_{\alpha}|^2 |v_c|^2] \mathbb{E}[|w_{\alpha}|^2 |w_c|^2] \\ &= \frac{1}{FD^2} \sum_{\alpha=1, \alpha \neq c}^{\chi} \sum_{c=1}^{\chi} \mathbb{E}[S_{\alpha}^2 S_c^2] \\ &= \frac{1}{FD^2} \left(\sum_{\alpha=1}^{\chi} \sum_{c=1}^{\chi} \mathbb{E}[S_{\alpha}^2 S_c^2] - \sum_{c=1}^{\chi} \mathbb{E}[S_c^4] \right) \\ &= \frac{1}{FD^2} \left(\sum_{\alpha=1}^{\chi} \sum_{c=1}^{\chi} \mathbb{E}[S_{\alpha}^2 S_c^2] - O(1/\sqrt{D}) \right) \\ &= \frac{1}{FD^2} \left(F \sum_{\alpha=1}^{\chi} \mathbb{E}[S_{\alpha}^2] - O(1/\sqrt{D}) \right) \\ &= \frac{1}{D^2} \left(\sum_{\alpha=1}^{\chi} \mathbb{E}[S_{\alpha}^2] - O(1/\sqrt{D}) \right) \\ &= \frac{F}{D^2} \left(1 - O(1/\sqrt{D}) \right). \end{aligned}$$

Case 3: $\alpha = \beta = c = d$. From Eq. (F30) and the first

row of the Table above, we have

$$\begin{aligned} g_{j,\chi,D} &= \frac{1}{F} \sum_{c=1}^{\chi} \mathbb{E}[S_c^4] \mathbb{E}[|v_c|^4] \mathbb{E}[|w_c|^4] \\ &= \frac{1}{F} \left(\frac{\beta + 2}{2\sqrt{D}(\sqrt{D} + 1)} \right)^2 \sum_{c=1}^{\chi} \mathbb{E}[S_c^4] \\ &\approx \frac{4}{D^2} \frac{\sum_{c=1}^{\chi} \mathbb{E}[S_c^4]}{F} \left(1 - \frac{2}{D^{1/2}} \right) \\ &= O(D^{-5/2}). \end{aligned} \quad (\text{F33})$$

We can now compute the desired result. First of all from Eq. (F29) and the above 3 cases we have

$$\mathbb{E} \sum_j \tilde{p}_j p_j = \frac{1}{D} + \frac{F}{D} + O(D^{-3/2}).$$

Therefore,

$$D \mathbb{E} \left[\sum_j \tilde{p}_j p_j \right] - 1 = F + O(1/\sqrt{D}), \quad (\text{F34})$$

which proves our result. \square

We now consider the special case of $\chi = 1$ where the approximate state $|\tilde{\psi}\rangle$ is taken to be a product state.

Corollary 1. When $\chi = 1$, then $D \mathbb{E} \left[\sum_j \tilde{p}_j p_j \right] - 1 = 3F + O(F/\sqrt{D})$.

Proof. In this case

$$\mathbb{E}[p_j \tilde{p}_j] = \sum_{\alpha, \beta=1}^{\sqrt{D}} \mathbb{E}[S_{\alpha} S_{\beta}] \mathbb{E}[v_{\alpha} w_{\alpha} \overline{v_{\beta} w_{\beta}} |v_1|^2 |w_1|^2] \quad (\text{F35})$$

The only non-zero contributions come from $\alpha = \beta = 1$ and $\alpha, \beta \geq 2$. We have

$$\begin{aligned} \mathbb{E}[p_j \tilde{p}_j] &= \mathbb{E}[S_1^2] \mathbb{E}[|v_1|^4 |w_1|^4] \\ &\quad + \sum_{\alpha, \beta=2}^{\sqrt{D}} \mathbb{E}[S_{\alpha} S_{\beta}] \mathbb{E}[v_{\alpha} w_{\alpha} \overline{v_{\beta} w_{\beta}} |v_1|^2 |w_1|^2] \\ &= F \mathbb{E}[|v_1|^4] \mathbb{E}[|w_1|^4] \\ &\quad + \sum_{\alpha=2}^{\sqrt{D}} \mathbb{E}[S_{\alpha}^2] \mathbb{E}[|v_{\alpha}|^2] \mathbb{E}[|w_{\alpha}|^2] \mathbb{E}[|v_1|^2] \mathbb{E}[|w_1|^2] \\ &= F \mathbb{E}[|v_1|^4] \mathbb{E}[|w_1|^4] + \frac{1}{D^2} (1 - F) \\ &= F \left(\frac{\beta + 2}{2\sqrt{D}(\sqrt{D} + 1)} \right)^2 + \frac{1}{D^2} (1 - F) \\ &= F \frac{4}{D^2} \frac{1}{(1 + 1/\sqrt{D})^2} + \frac{1}{D^2} (1 - F) \\ &= F \frac{4}{D^2} \left(1 - 2/\sqrt{D} \right) + \frac{1}{D^2} (1 - F) \\ &= \frac{3F}{D^2} + \frac{1}{D^2} + O(F D^{-5/2}). \end{aligned}$$

We conclude the desired final result

$$D \sum_j \mathbb{E}[p_j \tilde{p}_j] = 3F + 1 + O(F D^{-1/2}).$$

□

5. Quantifying entanglement with Clifford circuits

We derived an analytical and numerical bound on the fidelity of the tensor product approximation, Eqs. (F14) and (F15), which depend on the reduced purity. We now study the reduced purity growth rate in phase matched circuits (see SM C1). The average Pauli error between the fsim gates used in the experiment and the Clifford gate iSWAP⁻¹ is $\sim 1\%$. For the purposes of quantifying reduced purity growth we therefore approximate fsim gates with iSWAP⁻¹. The one-qubit gates are $Z^p X^{1/2} Z^{-p}$ with $p \in \{-1, -1/4, -1/2, \dots, 3/4\}$ [30]. We can study a related ensemble of Clifford circuits by reducing the parameter p of the one-qubit gates to the set $p \in \{-1, -1/2, -1, 1/2\}$. Note that the reduced purity produced by Clifford circuits is efficient to calculate numerically [31].

Consider the average purity of the reduced state $\langle\langle \text{tr } \rho_L^2 \rangle\rangle$, where ρ_L is the partial trace of $|\psi\rangle$ on the left qubits. We now show that layer by layer this average is the same for the random circuits and the corresponding Clifford circuits of the previous paragraph. One intuition why this might be true is that Clifford circuits are a two-design. Nevertheless, we are interesting in the growth rate, not the average over Clifford circuits. Therefore, we use a different technique.

First note that $\text{tr } \rho_L^2$ can be written as

$$\sum_{z_L} \langle z_L | \sum_{z_R} \langle z_R | \rho | z_R \rangle | z_L \rangle \otimes \langle z_L | \sum_{z_R} \langle z_R | \rho | z_R \rangle | z_L \rangle ,$$

where $\{z_L\}$ ($\{z_R\}$) is a basis for the left (right) patch. Therefore, this quantity can be calculated from two replicas of the output state of the circuit of interest $\rho \otimes \rho$. As shown in SM D and Ref. [10], for the circuits of interest, the average of an observable with two replicas can be calculated with a Markov chain describing the evolution of the density matrix in the basis of Pauli strings. If we denote the basis of normalized Pauli strings as $\{s\}$ we can write any operator as $\rho = \sum_s \text{tr}(\rho s) s$. It follows that

$$U \rho U^\dagger = \sum_s \text{tr}(\rho s) \sum_{s'} \text{tr}(s' U s U^\dagger) s' . \quad (\text{F36})$$

Using this relation repeatedly we reduce the evolution of a circuit to the evolution of gates over Pauli strings. Furthermore, the average over random circuits is composed of averages over the corresponding set $\{g\}$ of random gates. In the case of the evolution of two replicas the

elementary step is

$$\begin{aligned} \mathbb{E}_g[\sigma^\alpha \otimes \sigma^{\alpha'}] &= \\ \sum_{\beta, \beta'} \frac{1}{|g|} \sum_g \text{tr}(\sigma^\beta \otimes \sigma^{\beta'} g \otimes g \sigma^\alpha \otimes \sigma^{\alpha'} g^\dagger \otimes g^\dagger) \sigma^\beta \otimes \sigma^{\beta'} \end{aligned} \quad (\text{F37})$$

where the tensor product is between the two replicas, and each gate is the same for both replicas. The initial state of each qubit with two replicas is

$$|0\rangle \langle 0| \otimes |0\rangle \langle 0| = \frac{1+Z}{2} \otimes \frac{1+Z}{2} . \quad (\text{F38})$$

We obtain, both the Clifford and non-Clifford single-qubit gates above,

$$\mathbb{E}[II] = II \quad (\text{F39})$$

$$\mathbb{E}[IZ] = \mathbb{E}[ZI] = 0 \quad (\text{F40})$$

$$\mathbb{E}[ZZ] = \frac{1}{2}(XX + YY) \equiv \perp \quad (\text{F41})$$

where we also define the symbol \perp . For shorthand, we also introduce the notation $\mathbb{Z} = ZZ$ and $\mathbb{I} = II$. We also obtain, again for both the Clifford and non-Clifford gates,

$$\mathbb{E}[\perp] = \frac{1}{2}(\mathbb{Z} + \perp) . \quad (\text{F42})$$

Finally the transformation from applying iSWAP⁻¹ to two qubits in each replica gives

$$\mathbb{I}\mathbb{Z} \rightarrow \mathbb{Z}\mathbb{I} \quad (\text{F43})$$

$$\mathbb{I} \perp \rightarrow \perp \mathbb{Z} \quad (\text{F44})$$

$$\mathbb{Z}\mathbb{Z} \rightarrow \mathbb{Z}\mathbb{Z} \quad (\text{F45})$$

$$\perp \perp \rightarrow \perp \perp \quad (\text{F46})$$

$$\perp \mathbb{Z} \rightarrow \mathbb{I} \perp \quad (\text{F47})$$

Therefore the average purity of the reduced state $\langle\langle \rho_L \rangle\rangle$ is the same for both ensembles, as the transformations for the initial state of interest is the same for the average of Clifford and non-Clifford gates.

Entanglement is typically measured with the von Neumann entropy $-\rho_L \text{tr } \rho_L$. Using Jensen's inequality this can be bounded with the Rényi entropy

$$-\text{tr } \rho_L \log_2 \rho_L \geq -\log_2 \text{tr } \rho_L^2 . \quad (\text{F48})$$

The average Rényi entropy can be bounded with purity of the reduced states using Jensen's inequality as

$$-\langle\langle \log_2 \text{tr } \rho_L^2 \rangle\rangle \geq -\log_2 \langle\langle \text{tr } \rho_L^2 \rangle\rangle . \quad (\text{F49})$$

Figure 17 shows the reduced purity, as a function of the number of cycles, for different circuit sizes and cuts. Dashed lines are the reduced purity limit values (see Eq. F50). For Sycamore-70 (this work), the reduced purity is close to its limit value at cycle 10.

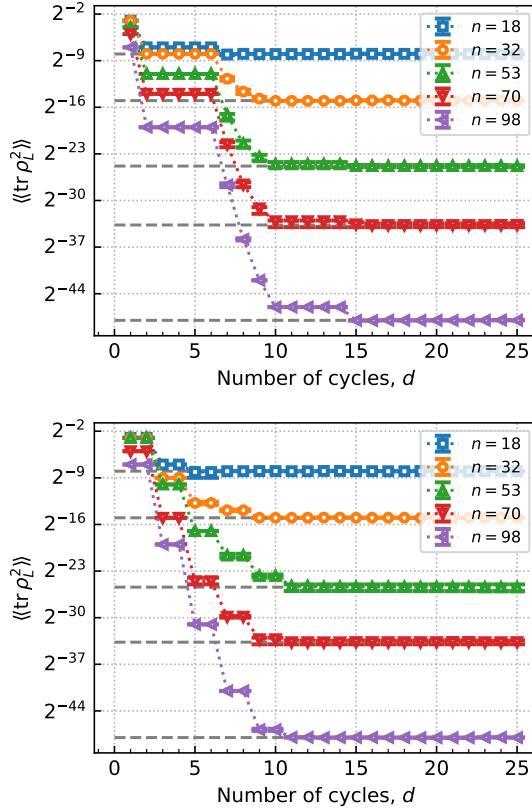


FIG. 17. The plots show the reduced purity as a function of the number of cycles, for different circuit sizes and cuts (diagonal cut for the top figure, and vertical cut for the bottom figure), using Clifford gates only. The dashed lines correspond to the reduced purity $\overline{\text{pur}}$ in the random Haar limit (see Eq. F50). For all the instances, the pattern ABCDCDAB is used.

6. Reduced purity and distribution of singular values

We will now show numerically that the reduced purity is a good witness for the distribution of singular values, which undergoes through a sharp transition to its limiting value. We first need to understand what is the expected reduced purity and the corresponding standard deviation for a Haar random state. In Sec. F 1 we gave the distribution of the normalized singular values $s = \sqrt{D_1}S$, where D_1 is the small Hilbert space dimension (between the halves in which the state is being divided). The expected purity is

$$\overline{\text{pur}} = \left\langle\left\langle \sum_{\alpha=1}^{D_1} S_\alpha^4 \right\rangle\right\rangle \simeq \frac{1}{D_1^2} \left\langle\left\langle \sum_{\alpha=1}^{D_1} s_\alpha^4 \right\rangle\right\rangle = \frac{1}{D_1} \langle\langle s_\alpha^4 \rangle\rangle . \quad (\text{F50})$$

The variance is

$$\begin{aligned} \text{Var}(\text{pur}) &= \text{Var} \left(\sum_{\alpha=1}^{D_1} S_\alpha^4 \right) \simeq \frac{1}{D_1^4} \sum_{\alpha=1}^{D_1} \text{Var}(s_\alpha^4) \\ &= \frac{1}{D_1^3} \text{Var}(s_\alpha^4) . \end{aligned} \quad (\text{F51})$$

Therefore, we can say that the reduced purity has converged to its limiting value at a given depth when

$$\frac{\text{tr} \rho_L^2 - \overline{\text{pur}}}{\sqrt{\text{Var}(\text{pur})}} \in O(1) \quad (\text{F52})$$

Note that the variance decreases exponentially.

Figure 18-Top shows the distance of the reduced purity in units of the standard deviation as a function of the number of cycles. As expected, the depth for which the reduced purity is exponentially close to its limit value increases with the system size. Figure 18-Bottom shows instead how the Kolmogorov-Smirnov p -value between the singular values S_α and the Haar random distribution of singular values (Eq. F10) transitions when the purity reaches its limiting value in units of standard deviation. As one can see, there is a sharp transition so that only once the reduced purity is appropriately close to its limit value, the distribution of S_α truly follows the distribution of singular values in the random Haar limit.

7. Bounding the approximate tensor representation performance for close simulations

Using Eqs. (F14) and (F15), it is possible to lower bound the required χ to achieve a target fidelity F for close simulations (see App. F 3). For our bounds, we split circuits C of m cycles in three parts of $|C_1| = m - 2$, $|C_M| = 4$ and $|C_2| = m - 2$ cycles respectively. Moreover, we assume that it is possible to compute $|\tilde{\Psi}_1\rangle$ and $|\tilde{\Psi}_2(x)\rangle$ with a single truncation each. While being unrealistic for any practical purpose, it allows us to find analytical and semi-analytical bounds since every realistic simulation would require more than one truncation.

Recalling that the final fidelity of a close simulation is $F = F_1 \overline{F}_2$, with F_1 and \overline{F}_2 being the fidelity of $|\tilde{\Psi}_1\rangle$ and the average fidelity $|\tilde{\Psi}_2(x)\rangle$ respectively, it is possible to get an estimate of the optimal bond dimension χ for a given target fidelity F as:

$$\chi_{\text{an}} = \frac{F}{\langle\langle \text{tr} \rho_L^2 \rangle\rangle}, \quad (\text{F53a})$$

$$\chi_{\text{nm}} = \frac{\mathcal{F}_\lambda^{-1}(\sqrt{F})}{\langle\langle \text{tr} \rho_L^2 \rangle\rangle} \geq \frac{\sqrt{F}}{\lambda_+^2 \langle\langle \text{tr} \rho_L^2 \rangle\rangle}, \quad (\text{F53b})$$

with $\lambda_+^2 \leq 2$ being the largest singular value, and χ_{an} and χ_{nm} being respectively the estimate for the bond dimension using either the analytical or the numerical bound. It is important to stress that the upper bounds

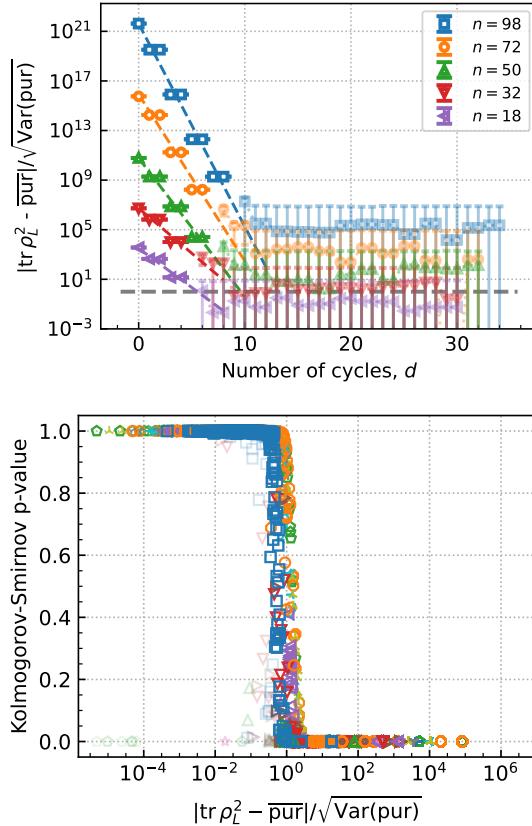


FIG. 18. (Top) Distance of the reduced purity from its limit value in units of the standard deviation as a function of cycles, using Clifford gates only. The dashed line correspond to 1. (Bottom) Kolmogorov-Smirnov p -value between the singular values S_α and the distribution of singular values for large depth, Eq. F10, as a function of the distance between the reduced purity and its limit value in units of standard deviation. Each point corresponds to a different circuits (with the number of qubits ranging from $n = 8$ and $n = 24$) at given fixed cycle. Lighter points correspond to datapoints outside the 90%. For all the instances, the pattern ABCDCDAB is used, and qubits are partitioned in two equal halves using a diagonal cut.

provided by Eqs. F53 are valid for arbitrary depths and bond dimensions χ , even if the quantum state has not yet reached the Porter-Thomas limit. For small target fidelity F , the ratio between χ_{an} and χ_{nm} becomes:

$$\frac{\chi_{\text{an}}}{\chi_{\text{nm}}} \approx \lambda_+^2 \sqrt{F}. \quad (\text{F54})$$

For a cut that split the qubits in two equal halves ($\lambda_+ = 2$), and for a target fidelity of $F = 10^{-4}$, one gets $\chi_{\text{nm}} \approx 25 \chi_{\text{an}}$, that is the numerical bound is only 25 times larger than the analytical bound. This is consistent with what we observe in Fig. 19.

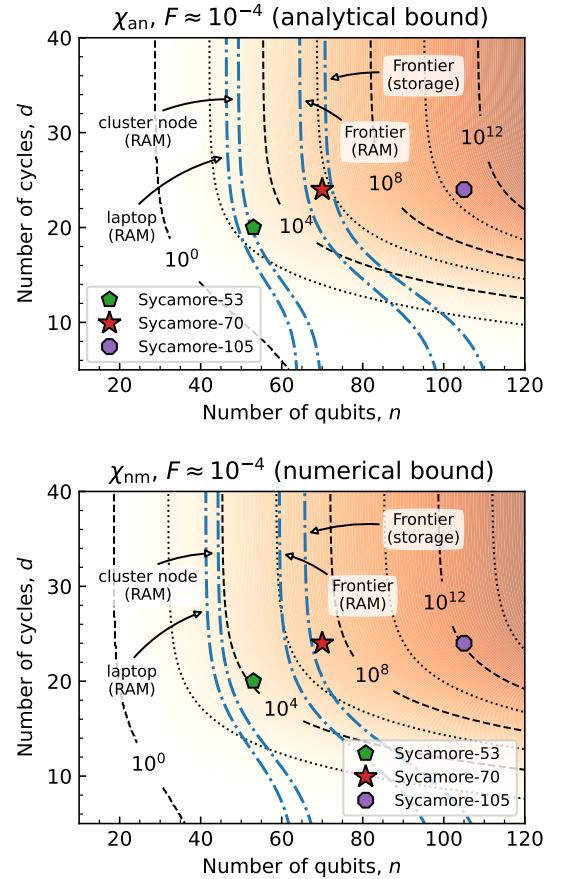


FIG. 19. Analytical (Top) and numerical (Bottom) upper bounds for the required bond dimension to achieve a target fidelity of $F = 10^{-4}$, by varying the number of qubits and cycles. The memory footprint is computed as the amount of memory required to store two `complex32` tensors of dimension $2^{n/2} \times \chi$. Laptop (RAM) = 32GB, cluster node (RAM) = 256GB, Frontier (RAM) = 9.2PB and Frontier (storage) = 700PB. The density map is obtained by averaging circuits with patterns ABCDCDAB/BADCDCBA and with diagonal/vertical cuts.

Appendix G: Client-certified randomness generation with RCS

Randomness is a valuable resource with many applications and is a key resource in much of modern cryptography. In classical physics, the outcome of any experiment can in principle be determined from the initial conditions, so there is no such thing as true randomness. On the other hand, quantum physical systems exhibit true randomness. The outcome of certain quantum processes is inherently random, meaning that no amount of prior information is sufficient to predict the outcome.

Client-certified randomness generation has been proposed as a potential application of RCS [32–34]. The proposed protocol works as follows. The client generates challenge random quantum circuits which she sends to an

untrusted server that operates a quantum processor. The server responds to each challenge by sending a requested number of bitstrings within a given short amount of time. When the server is honest, it produces the bitstrings by sampling from the circuit using the quantum processor, so the bitstrings contain entropy due to the inherent randomness of quantum measurements. The client can then pass the raw bitstrings through a randomness extractor to obtain random bits of higher quality, in the sense of being closer to the uniform distribution.

The client is able to gain confidence that the returned sample of bitstrings is consistent with executing the challenge circuits by performing statistical tests, such as XEB. For cryptographic certification of randomness, these tests need to account for the possibility that the quantum operator is adversarial. Such an adversary will try to construct a set of bitstrings that pass the statistical tests despite having low or no entropy. Challenge circuits must be executed with fidelity greater than an agreed value F . In principle, the client allots a sampling time sufficiently shorter than the necessary time to simulate the same sampling (number of bitstrings and fidelity) by all known classical algorithms using reasonable computing resources. This way, the client can gain confidence that the bitstrings were indeed obtained using a quantum computer, and therefore are a source of quantum randomness. Unfortunately, in this protocol, the client needs to perform classical simulations if she wishes to certify the quantum randomness using XEB. However, the client can do this simulation *a posteriori*, running classical computations for a much longer time. Furthermore, the client can in principle use a large number of challenge circuits and select only a subset of them for verification. This way the client can force an adversarial server to perform expensive simulations on a large number of circuits while only expending computing resources verifying a much smaller subset.

There exist a tension between the need for practical verification, which incurs an exponential cost in this proposal, and the requirement that an adversary could not pass the same test deterministically. Furthermore, "spoofing" is typically a factor of F cheaper than the verification [22]. The 70 qubit circuits presented in this work are currently too big to be verified with XEB. At the same time, the computational cost of classical algorithms keeps improving (see SM E), as well as the performance of implementations in specialized hardware [35]. In this work we do not resolve this tension, and we leave open the problem of finding an efficient verification protocol, perhaps along the line of cryptographically secure proposals [36, 37], or more near-term obfuscation techniques [38]. We nevertheless study how this protocol could work if this problem is resolved or if a client is willing to expend sufficient compute resources to gain enough confidence against a potential deterministic adversarial server.

1. Entropy estimation

The output of the protocol is produced by applying a randomness extractor to the output of the quantum computer; see Sec. G 4. A randomness extractor takes an input from the source with a given min-entropy, together with a uniformly random seed, and it outputs a near-uniformly random bitstring of length proportional to the input min-entropy. The min-entropy of a random variable X is defined as minus the log of the maximum probability:

$$\text{min-entropy} = - \max_x \log_2 (\Pr[X = x]). \quad (\text{G1})$$

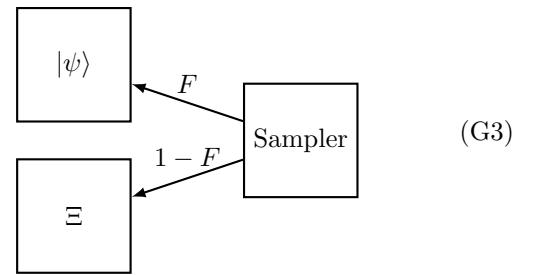
Below, we give bounds for the quantum min-entropy (see also Ref. [39]).

a. Entropy estimation for an honest server

The experimental output of a noisy quantum random circuit can be described by (see SM A)

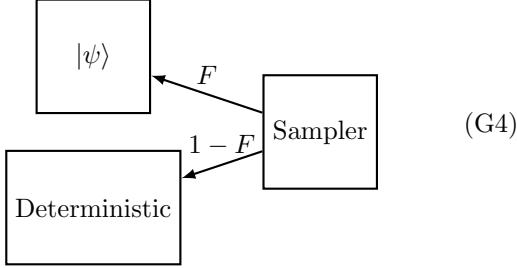
$$F |\psi\rangle\langle\psi| + (1 - F) \Xi, \quad (\text{G2})$$

where F is the experimental fidelity (probability of no error), $|\psi\rangle$ is the ideal output of the quantum circuit, and Ξ has trace one and is the result of errors. Measurement of this state can be interpreted as measuring the ideal quantum state $|\psi\rangle$ with probability F , and measuring the operator Ξ with probability $1 - F$. This is depicted in the following diagram:



For the purposes of quantum randomness generation, we take an adversarial approach with respect to the noise operator Ξ and consider it to be deterministic. The reason is that we are purely interested in the quantum entropy that is generated experimentally, and not in using potential "noise" or "errors" in the experiment as a source of entropy. Arguably, if we were willing to accept an entropy source based on "noise", there are simpler setups that do not require the use of a quantum processor. Furthermore, the potential entropy coming from the noise cannot be certified. Therefore, we model the

sampling as depicted in the next diagram:



Given the adversarial model above, the bitstring with the highest probability is the deterministic noise with probability $1 - F$. Therefore for a sample of size k the min-entropy is

$$\text{min-entropy} = -\log_2 ((1 - F)^k) \approx kF \quad (\text{G5})$$

It is possible to obtain a tighter bound by ignoring the very unlikely event that all outputs of the experiment correspond to the “noise” term, which we are treating as deterministic. The approach is to use the ε -min-entropy or smooth min-entropy, that is, we bound the min-entropy ignoring events with cumulative probability smaller than some suitable small ε .

In the simplified model given by (G4) within a sample of size k the expected number of bitstrings obtained from the ideal output $|\psi\rangle$ is kF with the variance $kF(1 - F)$. We wish to bound the probability of obtaining sufficiently many bitstrings from the ideal output. We now estimate this probability for obtaining a sequence of bitstrings from the ideal distribution up to a cumulative probability of $1 - \varepsilon$. Assuming that we are sampling from a quantum processor with experimental fidelity F , then we can choose a constant c_1 and upper-bound the probability of obtaining at least

$$q := kF - c_1 \sqrt{kF(1 - F)} \quad (\text{G6})$$

bitstrings from the *ideal* distribution, where c_1 is the number of standard deviations below the mean. Since the sample size is large enough (order of millions) we can use gaussianity where by $c_1 = 5$ implies that $\varepsilon = 1.5 \times 10^{-12}$ rendering the probability of success $1 - 1.5 \times 10^{-12}$.

Suppose that the distribution of the ideal output probabilities $p(s) = |\langle s|\psi\rangle|^2$ follows the Porter-Thomas distribution with the probability density function

$$f(x) = e^{-x}, \quad (\text{G7})$$

where $x = Dp(s)$ is the ideal bitstring probability scaled by the Hilbert space dimension $D = 2^n$. The average of minus log of the probability of one bitstring from the Porter-Thomas distribution is (see Eq. (A7))

$$-D^2 \int_0^\infty \log(p) e^{-Dp} p dp = \log(D) - 1 + \gamma, \quad (\text{G8})$$

where γ is Euler’s constant. Then minus the log of the probability of a sequence of q independent ideal bitstrings

is, by central limit theorem, a normal distribution with average $q(\log(D) - 1 + \gamma)$. The variance is upper-bounded by $q\pi^2/6$. Similar as above, we can choose a constant c_2 such that with high probability the ε -min-entropy is $q(\log(D) - 1 + \gamma) - c_2 \sqrt{q\pi^2/6}$. Putting it all together, we obtain the following lower-bound for the ε -min-entropy

$$q(\log(D) - 1 + \gamma) - c_2 \sqrt{\frac{q\pi^2}{6}}. \quad (\text{G9})$$

b. Correction to the min-entropy

The bound of Eq. (G9) represents the pure quantum min-entropy obtained from sampling a random quantum circuit. We now consider the situation in which a client has only black-box access (say via the cloud) to the quantum processor held by a server. We discuss deviations from the scenario of the previous section due to potential adversarial actions of the server, while still assuming that the server calls a quantum processor to obtain the output bitstrings.

In the previous section we bounded the number q of bitstrings obtained in a sample of size k using a quantum processor of fidelity F . An adversarial quantum server might be able to oversample sq bitstrings with $s \geq 1$ in the allotted time from the ideal quantum state before returning q bitstrings. The server can also rearrange the bitstrings in any predetermined way before returning them to the client. These operations lower the min-entropy and do not necessarily affect statistical tests such as the cross entropy. In order to bound the min-entropy of this multiset oversampling, we consider first a simplified model where the server samples from a uniform distribution of size D instead of the ideal quantum state.

We now give an expression for the probability of obtaining a given multiset S of size q when sampling sq times from the uniform distribution of D values. We can assume $q \ll D$ and that all the values in the set S are distinct. Let A_i denote the set of all sequences missing value i . We have

$$P(S) = 1 - \frac{|\bigcup_{i \in S} A_i|}{D^{sq}}. \quad (\text{G10})$$

Note that

$$\left| \bigcap_{i \in I} A_i \right| = (D - |I|)^{sq}. \quad (\text{G11})$$

Therefore, by the inclusion-exclusion principle, we have

$$\left| \bigcup_{i \in S} A_i \right| = \sum_{j=1}^q (-1)^{j-1} \binom{q}{j} (D - j)^{sq}, \quad (\text{G12})$$

and

$$P(S) = 1 - \sum_{j=1}^q (-1)^{j-1} \binom{q}{j} \left(\frac{D - j}{D} \right)^{sq}. \quad (\text{G13})$$

Although this expression is exact, note that all the terms have the same order in $1/D$, so it does not result in a compact estimate of the probability in the case of interest, $D \rightarrow \infty$.

We can also write different upper and lower bounds for $P(S)$. Let α denote a set of q indexes and B_α denote the set of words with the q given values in positions α . We first have

$$P(S) \leq \frac{\sum_\alpha |B_\alpha|}{D^{sq}}. \quad (\text{G14})$$

There are $q!$ ways in which the q values can appear in the α positions, and D^{sq-q} possible choices for the other $sq - q$ positions. Therefore

$$|B_\alpha| = q! D^{sq-q}. \quad (\text{G15})$$

There are sq chose q ways to choose α . Therefore

$$P(S) \leq \binom{sq}{q} \frac{q!}{D^q} = \frac{(sq)_q}{D^q}, \quad (\text{G16})$$

where

$$(sq)_q = \prod_{j=0}^{q-1} (sq - j) \quad (\text{G17})$$

This gives the following bound for the min-entropy

$$\text{min-entropy} \geq q \log D - \log((sq)_q). \quad (\text{G18})$$

We can obtain a related lower bound by considering the sets C_α including words with the q values of interest in positions α , and none of those values anywhere else. Then

$$P(S) \geq \frac{\sum_\alpha |C_\alpha|}{D^{sq}} \quad (\text{G19})$$

$$= \binom{sq}{q} \frac{q!(D-q)^{sq-q}}{D^{sq}} \quad (\text{G20})$$

$$= \frac{(sq)_q}{D^q} \left(1 - \frac{q}{D}\right)^{q(s-1)}. \quad (\text{G21})$$

Therefore, in the limit of $D \rightarrow \infty$, we have

$$P(S) = \frac{(sq)_q}{D^q} \left(1 - O\left(\frac{q^2 s}{D}\right)\right) \quad (\text{G22})$$

$$\text{min-entropy} = q \log D - \log((sq)_q) + O\left(\frac{q^2 s}{D}\right) \quad (\text{G23})$$

$$\simeq q \log D - q \log sq + q. \quad (\text{G24})$$

We have seen that multiset sampling can lower the min-entropy by a factor $\log((sq)_q)$. Applying this to the honest server min-entropy bound, Eq. (G9), gives a bound for the multiset sampling min-entropy

$$q(\log(D) - 1 + \gamma) - c_2 \sqrt{\frac{q\pi^2}{6}} - \log((sq)_q). \quad (\text{G25})$$

2. Repeated bitstrings

In the previous section we ignored the possibility of repeated bitstrings in the adversarial server sampling. We study this now. We denote the total sampling budget of the adversarial server (sq in the previous section) by β . We will see that the client can require the server to return unique bitstrings, and this has little effect in the linear XEB as long as $\beta \ll D$. An adversarial server can also postselect to bitstrings that appear at least twice to artificially boost the nominal ‘‘fidelity’’ as measured by XEB. We will see that this effect is negligible as long as $s \ll \sqrt{D/q}$.

a. Probabilities for repeated bitstrings

The probability that a bitstring j appears exactly c times is

$$p'_j(c) = \binom{\beta}{c} p_j^c (1 - p_j)^{\beta-c}. \quad (\text{G26})$$

For large enough sampling budget β , there may occur collisions, i.e., repeated strings. We can calculate the expected number M of strings appearing with each multiplicity c , and the corresponding ideal probability value A . In the following, we derive closed formulas up to first-order approximation, confirming the formulas (G44), (G50) conjectured in Ref. [39, App. D].

Lemma 1. *Assuming $D + \beta \gg c$, the expected number of bitstrings that appear exactly c times is*

$$M_{\beta,c} = \binom{\beta}{c} \frac{D^{1-c} c!}{\left(1 + \frac{\beta}{D}\right)^{c+1}} \left(1 + O\left(\sqrt{\frac{(2c)!}{D}}\right)\right). \quad (\text{G27})$$

Proof. The expected number of bitstrings that appear exactly c times is

$$M_{\beta,c} = \sum_j p'_j(c). \quad (\text{G28})$$

First note that

$$M_{\beta,c} = \sum_j p'_j(c) \quad (\text{G29})$$

$$= D \langle \langle p'(c) \rangle \rangle + O\left(\sqrt{D \text{Var}(p'(c))}\right), \quad (\text{G30})$$

where, as in App. A, we use the approximation that for large D the probabilities $p'_j(c)$ are i.i.d.

We can write

$$\langle \langle p'(c) \rangle \rangle = \binom{\beta}{c} I(\beta, c), \quad (\text{G31})$$

where $I(\beta, c)$ is the expectation value of $p^c(1-p)^{\beta-c}$. This can be calculated as

$$I(\beta, c) = \int_0^1 p^c(1-p)^{\beta-c} dF(p) \quad (\text{G32})$$

$$= \int_0^1 p^c(1-p)^{\beta-c}(D-1)(1-p)^{D-2} dp \quad (\text{G33})$$

$$= (D-1)c! \frac{(D+\beta-c-2)!}{(D+\beta-1)!} \quad (\text{G34})$$

$$= (D-1)c! \frac{1}{(D+\beta-1)_{c+1}}, \quad (\text{G35})$$

where the last expression uses a falling factorial in the denominator. Therefore

$$\langle\langle p'(c) \rangle\rangle = \binom{\beta}{c} \frac{(D-1)c!}{(D+\beta-1)_{c+1}}, \quad (\text{G36})$$

We are interested in the value for large D , so we can use the approximation

$$\langle\langle p'(c) \rangle\rangle \simeq \binom{\beta}{c} \frac{(D-1)c!}{\left(D+\beta-1-\frac{c}{2}\right)^{c+1}}. \quad (\text{G37})$$

This approximation is valid for

$$D + \beta \gg c, \quad (\text{G38})$$

which is always the case in the regime of parameters we are interesting in.

We can also estimate the variance

$$\frac{\text{Var}(p'(c))}{\binom{\beta}{c}^2} \quad (\text{G39})$$

$$= \frac{(D-1)(2c)!}{(D+2\beta-1-c)^{2c+1}} - \left(\frac{(D-1)c!}{(D+\beta-1-\frac{c}{2})^{c+1}} \right)^2 \quad (\text{G40})$$

$$= D^{-2c} \frac{(1-\frac{1}{D})(2c)!}{\left(1+2\frac{\beta}{D}-\frac{1}{D}-\frac{c}{D}\right)^{2c+1}} - D^{-2c} \left(\frac{(1-\frac{1}{D})c!}{\left(1+\frac{\beta}{D}-\frac{1}{D}-\frac{c}{2D}\right)^{c+1}} \right)^2. \quad (\text{G41})$$

Ignoring small terms we get

$$\text{Var}(p'(c)) = \binom{\beta}{c}^2 D^{-2c} ((2c)! - (c!)^2 + O(\beta/D)). \quad (\text{G42})$$

Keeping only the dominant term $(2c)!$ completes the proof of the lemma.

Note that we also ignore terms $O(1/D)$ and $O(c/D)$ for consistency with the fluctuations from the variance. \square

In Eq. (G27) we can use $\beta \gg c$ to write

$$\binom{\beta}{c} \simeq \frac{\left(\beta - \frac{c}{2}\right)^c}{c!}. \quad (\text{G43})$$

Plugging this back and ignoring again terms $O(1/D)$ and $O(c/D)$ we get

$$M_{b,c} \simeq D \frac{b^c}{(1+b)^{c+1}}, \quad (\text{G44})$$

where $b = \beta/D$.

We are also interested in the expected value of the simulated or ideal probability for the bistrings that are obtained exactly c times in a β -sample.

Lemma 2. *The expected value of the ideal probability for the bistrings that are obtained exactly c times is*

$$A_{\beta,c} = \frac{1}{D} \frac{c+1}{1+b}. \quad (\text{G45})$$

Proof. The probabilities of bitstrings conditioned on appearing exactly c times are proportional to $p'_j(c)$, normalized so that their sum is 1. That is, the conditional probabilities are $p'_j(c)/M_{b,c}$. Therefore, the expected value of the simulated probability conditioned on appearing c times has the expression

$$A_{\beta,c} = \frac{1}{M_{\beta,c}} \sum_j p'_j(c) p_j. \quad (\text{G46})$$

Using the same methodology as in Lemma 1 we have

$$A_{\beta,c} = \frac{\int_0^1 p^{c+1}(1-p)^{\beta-c} dF(p)}{\int_0^1 p^c(1-p)^{\beta-c} dF(p)} \quad (\text{G47})$$

$$= \frac{I(\beta+1, c+1)}{I(\beta, c)} \quad (\text{G48})$$

$$= \frac{(c+1)!}{c!} \frac{(D+\beta-1)_{c+1}}{(D+\beta)_{c+2}} \quad (\text{G49})$$

$$= \frac{1}{D} \frac{c+1}{1+b}. \quad (\text{G50})$$

\square

The expected number of unique bitsrings in a β -sample follows from Eq. (G44) and is given by the expression

$$M_\beta = \sum_{c=1}^{\infty} M_{\beta,c} = D \frac{\beta}{D+\beta}. \quad (\text{G51})$$

b. Linear cross-entropy with unique bitstrings

Following the same logic as in Eq. (G46), we can calculate the expected value of the linear cross entropy when

an honest server returns unique bitstrings. The probabilities of bitstrings conditioned on appearing at least one time are proportional to

$$p_j''(c) = \sum_{c=1}^{\infty} p_j'(c), \quad (\text{G52})$$

normalized so that their sum is 1. The corresponding linear cross entropy is

$$D \sum_j \frac{p_j''(c)}{M_{\beta}} p_j - 1 = \frac{D}{M_{\beta}} \sum_{c=1}^{\infty} A_{\beta,c} M_{\beta,c} - 1 \quad (\text{G53})$$

$$= \frac{2+b}{1+b} - 1 = \frac{1}{1+b}. \quad (\text{G54})$$

The expectation value of the linear cross entropy is 1 when allowing repeated bitstrings if sampling from a Haar random quantum state. Therefore, the perturbation to the linear cross entropy when requiring unique bitstrings can be ignored when $b \ll 1$ or, equivalently, $\beta \ll D$. Note that sampling with less fidelity results in a lower frequency of collisions.

c. Adversarial postselection of repetitions

Consider now the situation where an adversarial server is asked to return k unique bitstrings, but the server secretly oversamples many more bitstrings to take advantage of collisions. That is, the server can postselect bitstrings that appear at least twice, and therefore, in the ideal case of fidelity 1, have a higher expectation value for the simulated probability $DA_{\beta,2} \sim 3$, instead of the usual average simulated probability $\langle Dp \rangle = 2$. In this way, the server could pass the linear cross entropy test returning a smaller number of quantum generated bitstrings, that is, a sample with similar estimated fidelity but less quantum entropy.

Next we bound how many bitstrings can be oversampled with still a negligible effect in the estimated fidelity from linear cross entropy. In order to cover the case of an adversarial server with non-ideal fidelity $\phi < 1$, we consider an idealized model where errors are heralded. That is, we treat sampling sk bitstrings with fidelity ϕ as sampling $\beta = sq$ bitstrings with fidelity 1, where $q = \phi k$. The contribution to the linear cross entropy for bitstrings that appear $c = 2$ times is

$$\frac{D}{q} M_{\beta,2} A_{\beta,2} = \frac{D}{q} \frac{\beta^2}{D^2} 3(1 + O(\beta/D)) \quad (\text{G55})$$

$$= 2 \frac{s^2 q}{D} 3(1 + O(\beta/D)). \quad (\text{G56})$$

This effect is negligible for $s \ll \sqrt{D/q}$.

3. Additional statistical tests

We explained in the main text the conditions under which XEB is an estimator of fidelity, which is the main

test for experimental RCS (see also SM A). Ref. [6] also introduced the idea of checking the consistency between log and linear XEB, and a Kolmogorov-Smirnov test for the simulated probabilities of the experimental bitstrings. We now introduce two additional statistical tests which might be useful in an adversarial setting such as client-certified randomness generation.

a. Hamming distance filter

In order to sample from the output distribution of a quantum circuit one can use an independent tensor contraction per output bitstring using frugal rejection sampling (see SM E and Refs. [22, 23]). This results in a simulation runtime that scales linearly in the number of bitstrings sampled. Ref. [19] introduced a method to compute amplitudes of a large number of uncorrelated bitstrings with a much lower overhead than linear.

An adversarial server using tensor network contractions could avoid the remaining overhead from Ref. [19] using less tensor network contractions to calculate the probabilities of many bitstring with small Hamming distance between them, although this does not perform RCS (see for instance Ref. [40]). We now give a Hamming distance filter test which detects this pseudo-sampling.

We can approximate a Porter-Thomas sampling as a uniform sampling of bitstrings for the purpose of analyzing the Hamming distance between unique sampled bitstrings. We denote the distance between bitstrings j and k as h_{jk} . For fixed j , the distribution of the Hamming distance to other bitstrings is binomial with n the number of qubits and $p = 1/2$. As an example we can consider $n = 70$ and Hamming distance 15. The probability of $h_{jk} \leq 15$ is

$$p_h = \frac{1}{2^n} \sum_{c=0}^{15} \binom{70}{c} = 8.26 \cdot 10^{-7}. \quad (\text{G57})$$

The experimental readout measurement error has a bias which we can take into account. Let e_{01} bet the probability of measuring state 0 when the quantum state is 1 and e_{10} the probability of measuring state 1 when the quantum state is 0. This gives a bias $b = e_{01} - e_{10}$. The probability of sampling a 1 on a qubit is, on average, $p_b = (1 - b)/2$, while the probability of sampling a 0 is $1 - p_b$. The probability of obtaining a given Hamming distance between two bitstrings is therefore given by a binomial distribution with the slightly biased value of p_b , which is slightly higher than in the unbiased case.

For a given sample S with k bitstrings, we can eliminate sufficient bitstrings so that there are no pairs of bitstrings within Hamming distance less than some bound, such as 15. One way to do this is to process the bitstrings one by one in the sample S . For each bitstring, we eliminate all the other bitstrings at Hamming distance 15 or less. With this method, we keep more than half of the bitstrings if $k = 10^6$. Note that each random ordering

of bitstrings results in a different sub-sample. Therefore, this is equivalent to implementing bootstrapping in the initial sample. That is, we can repeat this sub-sampling a large number of times calculating the XEB fidelity estimator each time. The average of the XEB of all the sub-samples corresponds, in the honest case, to the sample average. We can do this for larger Hamming distances also.

In conclusion, with some small computational cost we can prevent a potential attack using a tensor network algorithm to calculate probabilities of sets bitstrings with small Hamming distance between them.

b. Statistical test of large probabilities

The value of the XEB fidelity estimator is higher if, instead of sampling, an adversarial server outputs the bitstrings with the highest simulated probabilities. This might be detected already by tests introduced in Ref. [6], such comparing linear and log XEB, or the Kolmogorov-Smirnov test. Here we give another option, namely using a truncated XEB fidelity estimator which ignores the bitstrings with simulated probability beyond some threshold t .

Consider the XEB estimator based on the function (see SM A)

$$f_t(p_j) := D p_j \mathbb{1}_{p_j \leq t/D} \quad (\text{G58})$$

where p_j is the simulated or ideal probability for bitstring j , $D = 2^n$ is the Hilbert space dimension, and $\mathbb{1}_{p_j \leq t}$ is an indicator function with value 1 if $p_j \leq t$ and value 0 in other case. As explained in SM A we can model the sampling probabilities of a quantum processor with fidelity F as

$$p_j^F = F p_j + \frac{1 - F}{D}. \quad (\text{G59})$$

The expectation value of the sampling with function (G58) is

$$\sum_j p_j^F D p_j \mathbb{1}_{p_j \leq t/D}. \quad (\text{G60})$$

Assuming that the simulated probabilities are distributed according to the Porter-Thomas or exponential distribution we have

$$\begin{aligned} \text{tXEB} &= \sum_j p_j^F D p_j \mathbb{1}_{p_j \leq t/D} \\ &= D \langle \langle p_j^F D p_j \mathbb{1}_{p_j \leq t/D} \rangle \rangle \end{aligned} \quad (\text{G61})$$

$$= D^2 \int_0^t (Fx + 1 - F) x e^{-x} dx \quad (\text{G62})$$

$$= F + 1 - e^{-t} (1 + t + (1 + t + t^2)F). \quad (\text{G63})$$

As with any other XEB fidelity estimator, we can estimate the value tXEB sampling bitstrings from an experimental implementation. This gives the tXEB fidelity

estimator

$$F = \frac{\text{tXEB} - 1 + e^{-t}(1 + t)}{1 - e^{-t}(1 + t + t^2)}. \quad (\text{G64})$$

Note that we are interested in the case $t \gtrsim 2$, which makes the denominator positive.

In order to calculate the variance of this estimators, we need the expectation value of the square of tXEB. This is

$$\begin{aligned} &\sum_j p_j^F (D p_j \mathbb{1}_{p_j \leq t/D})^2 \\ &= D^2 \int_0^t (Fx + 1 - F)x^2 e^{-x} dx. \end{aligned} \quad (\text{G65})$$

This integral can be calculated analytically to obtain an expression for the variance of the corresponding estimator of fidelity. For simplicity, we only give the variance in the limit $F \rightarrow 0$, which is

$$\text{VAR}(\text{tXEB}) \simeq \frac{1 - e^{-t}t^2 - e^{-2t}(1 + 2t + t^2)}{(1 - e^{-t}(1 + t + t^2))^2}. \quad (\text{G66})$$

Table I shows the variance for different values of the truncation parameter. We see that in an experimental sample we can ignore all bitstrings with ideal probabilities $\geq 4/D$ without affecting much the variance of the corresponding tXEB estimator. This gives another statistical test sensitive to a potential adversary which postselects bitstrings with unusually large ideal probabilities.

$\text{VAR}(F)$	t
1.00557	10.
1.06288	7.
1.32601	5.
1.84472	4.
4.11632	3.
10.144	2.5
105.982	2.

TABLE I. Variance of the truncated XEB estimate of F against the truncation parameter t .

4. Randomness extractor

Randomness extractors are functions that convert bits from a weak source of randomness into near-uniform random bits [41]. In our protocol we apply a randomness extractor to the output of a quantum computer, which contains intrinsic randomness but is not uniformly distributed. In this section, we describe the randomness extractor we implemented and present some benchmark results of its running time.

For general sources of randomness, randomness extraction is only possible if the extractor is also given a small uniformly random input seed as a catalyst.

A weak random source has a distribution over $\{0, 1\}^n$ which has some entropy. The most conservative estimate of the unpredictability of the outcomes is given by the min-entropy or equivalently the ∞ -Rényi entropy:

Definition 1. Let X be a probability distribution on the hyper-cube $\{0, 1\}^n$, and let p_x be the probability of the string $x \in \{0, 1\}^n$. The minimum entropy of X is

$$\min_x (-\log_2 p_x) = -\max_x \log_2 p_x = -\log_2 \max_x p_x$$

For an n -bit distribution X with min-entropy k , we say that X is an (n, k) distribution.

We now formally define an extractor function. Let $\text{Ext} : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$ be the function that takes as input samples from an (n, k) distribution X and a uniformly random d -bit string seed, and outputs an m -bit string that is ε -close to uniform. We say that the extractor is (k, ε) if the output is ε close to uniform random, where ε is the statistical distance. In extracting randomness from random variables from the knowledge of just a lower-bound on the min-entropy, a key concept is k -source.

Definition 2. A random variable X is called a k -source if its min-entropy is at least k . That is, $\Pr[X = x] \geq 2^{-k}$.

a. Trevisan's extractor and HMAC

We implemented a randomness extractor based on Trevisan's construction [42]. Since this extractor is somewhat slow, we describe in App. G 4c an alternative construction using the cryptographic primitive hash-based message authentication code (HMAC) that is more efficient, though it is a heuristic, not a theoretically proven extractor like Trevisan's.

We implemented Trevisan's extractor following primarily the construction of Raz, Reingold, and Vadhan [43] with some optimizations from [44]. The initial extractor was implemented entirely in Python, and profiling was used to identify bottlenecks, which were then rewritten in C++. In our case, over 99% of the running time was spent evaluating polynomials in a subroutine that computed Reed-Solomon codes. This code was migrated to a C++ library using NTL [45].

For a fixed ε , the extractor uses $O(\log^2 n)$ additional random bits. The theoretical optimal seed size for any seeded extractor, is $\log(n - k) + 2 \log(2/\varepsilon) + O(1)$. For a fixed seed size, min-entropy, and ε , the extractor takes time linear in the size n of the input. However, our inputs are several orders of magnitude larger than those considered by previous papers and previous benchmarked implementations of Trevisan's extractor, such as [44] and [46].

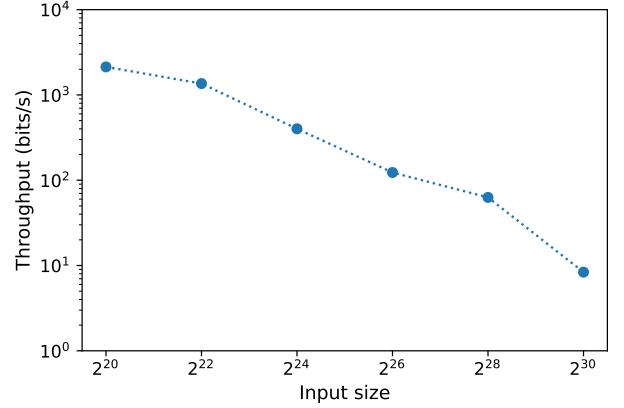


FIG. 20. Throughput of the Trevisan randomness extractor for various input sizes, when the output length is 4096 bits. We used 64 threads. Each data point is the average of the values obtained from 10 runs, and there are error bars of one standard deviation (too small to see).

b. Benchmark results

We tested the performance of our implementation of Trevisan's randomness extractor on various input sizes ranging from 2^{20} bits to 2^{30} bits. We used a workstation with an Intel Xeon Gold 6154 3.00GHz CPU which has 18 cores, each with 4 threads. We used 64 threads for our benchmarking.

Part of the running time of our extractor is spent in passing the input data from Python to C++. This conversion occurred at a rate of about 44 Mbit/s. Once this conversion has taken place, the extractor produces output bits at a constant rate, which we term the *throughput*, when the total length of the output is fixed. In Figure 20, we plot the throughput for the various input sizes when the output length is fixed to 4096 bits. At the input size of 2^{30} , the throughput was 8.4 bits/s. As an example, at the input size of 2^{30} , the Python to C++ conversion took about 24 seconds, while the rest of the extraction took about 490 seconds to produce the 4096 bits of output. While this throughput is slow compared to, say, the computation of a hash function like SHA-512, it is sufficient for many purposes. For example, a high-security cryptographic key requiring 256 bits of entropy may be used for days or weeks before needing to be refreshed.

c. A faster randomness extractor using HMAC

Our implementation of Trevisan's randomness extractor suffers from the disadvantage of being quite slow. In practice, theoretically proven randomness extractors are rarely used, with common efficient heuristic cryptographic primitives such as HMAC often used instead [47, 48]. In this appendix, we explain how one can use

an HMAC to construct a heuristic randomness extractor that works in our setting. Besides being a heuristic, our construction suffers from the disadvantage of requiring a rather large seed size (linear in the size of the output). Nevertheless, it may be of more practical use in some situations than the Trevisan extractor.

The main obstacle to overcome in using an HMAC for randomness extraction is that the output length is limited. For example, a SHA512-based HMAC will only output 512 bits, even when the input has many more bits of min-entropy. Here, we show, using Lemma 6.38 in [41], that one can extend the output length of a randomness extractor. The lemma says the following:

Lemma 3. (Lemma 6.38 in [41]): Suppose $\text{Ext}_1: \{0,1\}^n \times \{0,1\}^{d_1} \rightarrow \{0,1\}^{m_1}$ is a (k_1, ε_1) -extractor and $\text{Ext}_2: \{0,1\}^n \times \{0,1\}^{d_2} \rightarrow \{0,1\}^{m_2}$ is a (k_2, ε_2) -extractor for $k_2 = k_1 - m_1 - \log(1/\varepsilon_3)$. Then $\text{Ext}' : \{0,1\}^n \times \{0,1\}^{d_1+d_2} \rightarrow \{0,1\}^{m_1+m_2}$ defined by $\text{Ext}'(x, (y_1, y_2)) = (\text{Ext}_1(x, y_1), \text{Ext}_2(x, y_2))$ is a $(k_1, \varepsilon_1 + \varepsilon_2 + \varepsilon_3)$ -extractor.

Changing notation, letting $\text{Ext}(X, S) := \text{Ext}_1 = \text{Ext}_2$, $m := m_1 = m_2$, and $\varepsilon := \varepsilon_1 = \varepsilon_2$; and renaming the independent variable ε_3 as ε_1 we can restate this lemma as: if $\text{Ext}(X, S) = Y$ is a (k, ε) -extractor with an m -bit output, then $(\text{Ext}(X, S_1), \text{Ext}(X, S_2))$ is a $(k + m + \log(1/\varepsilon_1), 2\varepsilon + \varepsilon_1)$ -extractor with a $2m$ -bit output.

Let us define U_d to be a uniform random seed of size d bits. As explained in [41], $k_2 = k_1 - m_1 - \log(1/\varepsilon_3)$ in Lemma 3 arises because if one conditions a k_1 -source on the output of $\text{Ext}_1(X, U_{d_1})$, then the source still has a conditional min-entropy of at least $k_1 - m_1 - \log(1/\varepsilon_3) = k_2$ except with probability ε_3 . Therefore, $\text{Ext}_2(X, U_{d_2})$ can extract an additional m_2 almost-uniform bits. We can also ensure that $\text{Ext}_2(X, U_{d_2})$ can extract an additional m_2 almost-uniform bits by instead requiring X to be a $(k_2 + m_1 + \log(1/\varepsilon_3))$ -source.

This analysis can be recursively applied.

$$\begin{aligned} \text{Ext}''(X, (S_1, S_2, S_3, S_4)) \\ \equiv (\text{Ext}(X, S_1), \text{Ext}(X, S_2), \text{Ext}(X, S_3), \text{Ext}(X, S_4)) \end{aligned} \quad (\text{G67})$$

can be considered to be the combination of two $(k + m + \log(1/\varepsilon_1), 2\varepsilon + \varepsilon_1)$ -extractors:

- the first $(k + m + \log(1/\varepsilon_1), 2\varepsilon + \varepsilon_1)$ -extractor is $(\text{Ext}(X, S_1), \text{Ext}(X, S_2))$ and
- the second $(k + m + \log(1/\varepsilon_1), 2\varepsilon + \varepsilon_1)$ -extractor is $(\text{Ext}(X, S_3), \text{Ext}(X, S_4))$

Thus, selecting a new ε_2 , $\text{Ext}''(X, (S_1, S_2, S_3, S_4))$ is a $(k' + m' + \log(1/\varepsilon_2), 2\varepsilon' + \varepsilon_2)$ -extractor, where

- $k' = k + m + \log(1/\varepsilon_1)$,
- $m' = 2m$, and
- $\varepsilon' = 2\varepsilon + \varepsilon_1$.

So we get a $\left(k + 3m + \log\left(\frac{1}{\varepsilon_1}\right) + \log\left(\frac{1}{\varepsilon_2}\right), 4\varepsilon + 2\varepsilon_1 + \varepsilon_2\right)$ -extractor.

In general, to output $2^t m$ bits, we can construct an extractor

$$\begin{aligned} \text{Ext}^t(X, (S_1, S_2, \dots, S_{2^t})) \\ \equiv (\text{Ext}(X, S_1), \text{Ext}(X, S_2), \dots, \text{Ext}(X, S_{2^t})). \end{aligned} \quad (\text{G68})$$

This would lead to the following extractor

$$\left(k + (2^t - 1)m + \sum_{i=1}^t \log(1/\varepsilon_i), 2^t \varepsilon + \sum_{i=1}^t 2^{t-i} \varepsilon_i\right)$$

This analysis demonstrates that given sufficient min-entropy in the input X , we can repeatedly apply the same randomness extractor with a fresh seed to extract the desired number of output bits that are statistically close to uniform.

Google Quantum AI and Collaborators

A. Morvan^{1,‡}, B. Villalonga^{1,‡}, X. Mi^{1,‡}, S. Mandrà^{1, 2, 3,‡}, A. Bengtsson¹, P. V. Klimov¹, Z. Chen¹, S. Hong¹, C. Erickson¹, I. K. Drozdov^{1, 4}, J. Chau¹, G. Laun¹, R. Movassagh¹, A. Asfaw¹, L. T.A.N. Brandão⁵, R. Peralta⁵, D. Abanin¹, R. Acharya¹, R. Allen¹, T. I. Andersen¹, K. Anderson¹, M. Ansmann¹, F. Arute¹, K. Arya¹, J. Atalaya¹, J. C. Bardin^{1, 6}, A. Bilmes¹, G. Bortoli¹, A. Bourassa¹, J. BovaIRD¹, L. Brill¹, M. Broughton¹, B. B. Buckley¹, D. A. Buell¹, T. Burger¹, B. Burkett¹, N. Bushnell¹, J. Campero¹, H.-S. Chang¹, B. Chiaro¹, D. Chik¹, C. Chou¹, J. Cogan¹, R. Collins¹, P. Conner¹, W. Courtney¹, A. L. Crook¹, B. Curtin¹, D. M. Debroy¹, A. Del Toro Barba¹, S. Demura¹, A. Di Paolo¹, A. Dunsworth¹, L. Faoro¹, E. Farhi¹, R. Fatemi¹, V. S. Ferreira¹, L. Flores Burgos¹, E. Forati¹, A. G. Fowler¹, B. Foxen¹, G. Garcia¹, É. Genois¹, W. Giang¹, C. Gidney¹, D. Gilboa¹, M. Giustina¹, R. Gosula¹, A. Grajales Dau¹, J. A. Gross¹, S. Habegger¹, M. C. Hamilton^{1, 7}, M. Hansen¹, M. P. Harrigan¹, S. D. Harrington¹, P. Heu¹, M. R. Hoffmann¹, T. Huang¹, A. Huff¹, W. J. Huggins¹, L. B. Ioffe¹, S. V. Isakov¹, J. Iveland¹, E. Jeffrey¹, Z. Jiang¹, C. Jones¹, P. Juhas¹, D. Kafri¹, T. Khattar¹, M. Khezri¹, M. Kieferová^{1, 8}, S. Kim¹, A. Kitaev¹, A. R. Klots¹, A. N. Korotkov^{1, 9}, F. Kostritsa¹, J. M. Kreikebaum¹, D. Landhuis¹, P. Laptev¹, K.-M. Lau¹, L. Laws¹, J. Lee^{1, 10}, K. W. Lee¹, Y. D. Lensky¹, B. J. Lester¹, A. T. Lill¹, W. Liu¹, A. Locharla¹, F. D. Malone¹, O. Martin¹, S. Martin¹, J. R. McClean¹, M. McEwen¹, K. C. Miao¹, A. Mieszala¹, S. Montazeri¹, W. Mruczkiewicz¹, O. Naaman¹, M. Neeley¹, C. Neill¹, A. Nersisyan¹, M. Newman¹, J. H. Ng¹, A. Nguyen¹, M. Nguyen¹, M. Yuezhen Niu¹, T. E. O'Brien¹, S. Omonije¹, A. Opremcak¹, A. Petukhov¹, R. Potter¹, L. P. Pryadko¹¹, C. Quintana¹, D. M. Rhodes¹, C. Rocque¹, P. Roushan¹, N. C. Rubin¹, N. Saei¹, D. Sank¹, K. Sankaragomathi¹, K. J. Satzinger¹, H. F. Schurkus¹, C. Schuster¹, M. J. Shearn¹, A. Shorter¹, N. Shutty¹, V. Shvarts¹, V. Sivak¹, J. Skrzyni¹, W. C. Smith¹, R. D. Somma¹, G. Sterling¹, D. Strain¹, M. Szalay¹, D. Thor¹, A. Torres¹, G. Vidal¹, C. Vollgraff Heidweiller¹, T. White¹, B. W. K. Woo¹, C. Xing¹, Z. J. Yao¹, P. Yeh¹, J. Yoo¹, G. Young¹, A. Zalcman¹, Y. Zhang¹, N. Zhu¹, N. Zobrist¹, E. G. Rieffel², R. Biswas², R. Babbush¹, D. Bacon¹, J. Hilton¹, E. Lucero¹, H. Neven¹, A. Megrant¹, J. Kelly¹, I. Aleiner¹, V. Smelyanskiy¹, K. Kechedzhi^{1, §}, Y. Chen^{1, §}, S. Boixo^{1, §},

¹ Google Research² Quantum Artificial Intelligence Laboratory, NASA Ames Research Center, Moffett Field, California 94035, USA³ KBR, 601 Jefferson St., Houston, TX 77002, USA⁴ Department of Physics, University of Connecticut, Storrs, CT⁵ National Institute of Standards and Technology (NIST), USA⁶ Department of Electrical and Computer Engineering, University of Massachusetts, Amherst, MA⁷ Department of Electrical and Computer Engineering, Auburn University, Auburn, AL⁸ QSI, Faculty of Engineering and Information Technology, University of Technology Sydney, NSW, Australia⁹ Department of Electrical and Computer Engineering, University of California, Riverside, CA¹⁰ Department of Chemistry, Harvard University, Boston, NY¹¹ Department of Physics and Astronomy, University of California, Riverside, CA[‡] These authors contributed equally to this work.[§] Corresponding author: boixo@google.com[§] Corresponding author: bryanchen@google.com[§] Corresponding author: kostyantyn@google.com

-
- [1] W. K. Wootters, Random quantum states, *Foundations of Physics* **20**, 1365 (1990).
- [2] C. M. Caves, Measures and volumes for spheres, the probability simplex, projective hilbert space, and density operators, Unpublished (2001).
- [3] D. Petz and J. Réffy, On asymptotics of large haar distributed unitary matrices, *Periodica Mathematica Hungarica* **49**, 103 (2004).
- [4] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, M. J. Bremner, J. M. Martinis, and H. Neven, Characterizing quantum supremacy in near-term devices, *Nature Physics* **14**, 595 (2018).
- [5] K. Zyczkowski and H.-J. Sommers, Induced measures in the space of mixed quantum states, *Journal of Physics A: Mathematical and General* **34**, 7111 (2001).
- [6] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandaõ, D. A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M. P. Harrigan, M. J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T. S. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P. V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandrà, J. R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michelsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Y. Niu, E. Ostby, A. Petukhov, J. C. Platt, C. Quintana, E. G. Rieffel, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, K. J. Sung, M. D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven, and J. M. Martinis, Quantum supremacy using a programmable superconducting processor, *Nature* **574**, 505 (2019).
- [7] R. Barends, C. M. Quintana, A. G. Petukhov, Y. Chen, D. Kafri, K. Kechedzhi, R. Collins, O. Naaman, S. Boixo, F. Arute, K. Arya, D. Buell, B. Burkett, Z. Chen, B. Chiaro, A. Dunsworth, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M. P. Harrigan, M. J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T. S. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P. V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandrà, J. R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michelsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Y. Niu, E. Ostby, A. Petukhov, J. C. Platt, C. Quintana, E. G. Rieffel, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, K. J. Sung, M. D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven, and J. M. Martinis, Quantum supremacy using a programmable superconducting processor, *Nature* **574**, 505 (2019).

- ney, M. Giustina, R. Graff, T. Huang, E. Jeffrey, J. Kelly, P. V. Klimov, F. Kostritsa, D. Landhuis, E. Lucero, M. McEwen, A. Megrant, X. Mi, J. Mutus, M. Neeley, C. Neill, E. Ostby, P. Roushan, D. Sank, K. J. Satzinger, A. Vainsencher, T. White, J. Yao, P. Yeh, A. Zalcman, H. Neven, V. N. Smelyanskiy, and J. M. Martinis, Diabatic gates for frequency-tunable superconducting qubits, *Phys. Rev. Lett.* **123**, 210501 (2019).
- [8] C. Neill, T. McCourt, X. Mi, Z. Jiang, M. Y. Niu, W. Mruczkiewicz, I. Aleiner, F. Arute, K. Arya, J. Atalaya, R. Babbush, J. C. Bardin, R. Barends, A. Bengtsson, A. Bourassa, M. Broughton, B. B. Buckley, D. A. Buell, B. Burkett, N. Bushnell, J. Campero, Z. Chen, B. Chiaro, R. Collins, W. Courtney, S. Demura, A. R. Derk, A. Dunsworth, D. Eppens, C. Erickson, E. Farhi, A. G. Fowler, B. Foxen, C. Gidney, M. Giustina, J. A. Gross, M. P. Harrigan, S. D. Harrington, J. Hilton, A. Ho, S. Hong, T. Huang, W. J. Huggins, S. V. Isakov, M. Jacob-Mitos, E. Jeffrey, C. Jones, D. Kafri, K. Kechedzhi, J. Kelly, S. Kim, P. V. Klimov, A. N. Korotkov, F. Kostritsa, D. Landhuis, P. Laptev, E. Lucero, O. Martin, J. R. McClean, M. McEwen, A. Megrant, K. C. Miao, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, M. Newman, T. E. O'Brien, A. Opremcak, E. Ostby, B. Pató, A. Petukhov, C. Quintana, N. Redd, N. C. Rubin, D. Sank, K. J. Satzinger, V. Shvarts, D. Strain, M. Szalay, M. D. Trevithick, B. Villalonga, T. C. White, Z. Yao, P. Yeh, A. Zalcman, H. Neven, S. Boixo, L. B. Ioffe, P. Roushan, Y. Chen, and V. Smelyanskiy, Accurately computing the electronic properties of a quantum ring, *Nature* **594**, 508 (2021).
- [9] P. V. Klimov, J. Kelly, J. M. Martinis, and H. Neven, The snake optimizer for learning quantum processor control parameters (2020), arXiv:2006.04594 [quant-ph].
- [10] X. Mi, P. Roushan, C. Quintana, S. Mandrà, J. Marshall, C. Neill, F. Arute, K. Arya, J. Atalaya, R. Babbush, *et al.*, Information scrambling in quantum circuits, *Science* **374**, 1479 (2021).
- [11] X. Gao, M. Kalinowski, C.-N. Chou, M. D. Lukin, B. Barak, and S. Choi, Limitations of linear cross-entropy as a measure for quantum advantage, arXiv preprint arXiv:2112.01657 (2021).
- [12] A. M. Dalzell, N. Hunter-Jones, and F. G. S. L. Brandão, Random quantum circuits anticoncentrate in log depth, *PRX Quantum* **3**, 010333 (2022).
- [13] I. L. Markov and Y. Shi, Simulating quantum computation by contracting tensor networks, *SIAM Journal on Computing* **38**, 963 (2008).
- [14] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, and H. Neven, Simulation of low-depth quantum circuits as complex undirected graphical models, arXiv preprint arXiv:1712.05384 (2017).
- [15] J. Gray and G. K. Chan, Hyper-optimized compressed contraction of tensor networks with arbitrary geometry, arXiv:2206.07044 (2022).
- [16] C. Huang, F. Zhang, M. Newman, J. Cai, X. Gao, Z. Tian, J. Wu, H. Xu, H. Yu, B. Yuan, *et al.*, Classical simulation of quantum supremacy circuits, arXiv preprint arXiv:2005.06787 (2020).
- [17] G. Kalachev, P. Panteleev, and M.-H. Yung, Multi-tensor contraction for xeb verification of quantum circuits, arXiv preprint arXiv:2108.05665 (2021).
- [18] G. Kalachev, P. Panteleev, P. Zhou, and M.-H. Yung, Classical sampling of random quantum circuits with bounded fidelity, arXiv preprint arXiv:2112.15083 (2021).
- [19] F. Pan, K. Chen, and P. Zhang, Solving the sampling problem of the sycamore quantum circuits, *Physical Review Letters* **129**, 090502 (2022).
- [20] Y. Liu, Y. Chen, C. Guo, J. Song, X. Shi, L. Gan, W. Wu, W. Wu, H. Fu, X. Liu, *et al.*, Validating quantum-supremacy experiments with exact and fast tensor network contraction, arXiv preprint arXiv:2212.04749 (2022).
- [21] J. Chen, F. Zhang, C. Huang, M. Newman, and Y. Shi, Classical simulation of intermediate-size quantum circuits, arXiv preprint arXiv:1805.01450 (2018).
- [22] I. L. Markov, A. Fatima, S. V. Isakov, and S. Boixo, Quantum supremacy is both closer and farther than it appears, arXiv preprint arXiv:1807.10749 (2018).
- [23] B. Villalonga, S. Boixo, B. Nelson, C. Henze, E. Rieffel, R. Biswas, and S. Mandrà, A flexible high-performance simulator for verifying and benchmarking quantum circuits implemented on real hardware, *npj Quantum Information* **5**, 86 (2019).
- [24] Y. Wu, W.-S. Bao, S. Cao, F. Chen, M.-C. Chen, X. Chen, T.-H. Chung, H. Deng, Y. Du, D. Fan, M. Gong, C. Guo, C. Guo, S. Guo, L. Han, L. Hong, H.-L. Huang, Y.-H. Huo, L. Li, N. Li, S. Li, Y. Li, F. Liang, C. Lin, J. Lin, H. Qian, D. Qiao, H. Rong, H. Su, L. Sun, L. Wang, S. Wang, D. Wu, Y. Xu, K. Yan, W. Yang, Y. Yang, Y. Ye, J. Yin, C. Ying, J. Yu, C. Zha, C. Zhang, H. Zhang, K. Zhang, Y. Zhang, H. Zhao, Y. Zhao, L. Zhou, Q. Zhu, C.-Y. Lu, C.-Z. Peng, X. Zhu, and J.-W. Pan, Strong quantum computational advantage using a superconducting quantum processor, *Phys. Rev. Lett.* **127**, 180501 (2021).
- [25] Q. Zhu, S. Cao, F. Chen, M.-C. Chen, X. Chen, T.-H. Chung, H. Deng, Y. Du, D. Fan, M. Gong, C. Guo, C. Guo, S. Guo, L. Han, L. Hong, H.-L. Huang, Y.-H. Huo, L. Li, N. Li, S. Li, Y. Li, F. Liang, C. Lin, J. Lin, H. Qian, D. Qiao, H. Rong, H. Su, L. Sun, L. Wang, S. Wang, D. Wu, Y. Wu, Y. Xu, K. Yan, W. Yang, Y. Yang, Y. Ye, J. Yin, C. Ying, J. Yu, C. Zha, C. Zhang, H. Zhang, K. Zhang, Y. Zhang, H. Zhao, Y. Zhao, L. Zhou, C.-Y. Lu, C.-Z. Peng, X. Zhu, and J.-W. Pan, Quantum computational advantage via 60-qubit 24-cycle random circuit sampling, *Science Bulletin* **67**, 240 (2022).
- [26] Y. Zhou, E. M. Stoudenmire, and X. Waintal, What limits the simulation of quantum computers?, *Physical Review X* **10**, 041038 (2020).
- [27] T. Ayral, T. Louvet, Y. Zhou, C. Lambert, E. M. Stoudenmire, and X. Waintal, A density-matrix renormalisation group algorithm for simulating quantum circuits with a finite fidelity, arXiv:2207.05612 (2022).
- [28] V. A. Marčenko and L. A. Pastur, Distribution of eigenvalues for some sets of random matrices, *Mathematics of the USSR-Sbornik* **1**, 457 (1967).
- [29] R. Movassagh and A. Edelman, Isotropic entanglement, arXiv preprint arXiv:1012.5039 (2010).
- [30] We study the circuit ensemble consisting of random choices of one-qubit gates $Z^p X^{1/2} Z^{-p}$ with $p \in \{-1, -1/4, -1/2, \dots, 3/4\}$ and the two-qubit gate $iSWAP^{-1}$. We obtain the same ensemble if use $iSWAP$ instead of $iSWAP^{-1}$. This follows from $iSWAP^{-1} = iSWAP \cdot (Z \otimes Z) = (Z \otimes Z) \cdot iSWAP$ and the fact that

- the set $\{ZZ^p X^{1/2} Z^{-p}\}$ is the same as $\{Z^p X^{1/2} Z^{-p} Z\}$. Therefore we can move Z gates between layers as we transform iSWAP $^{-1}$'s to iSWAP's.
- [31] K. M. Audenaert and M. B. Plenio, Entanglement on mixed stabilizer states: normal forms and reduction procedures, *New Journal of Physics* **7**, 170 (2005).
 - [32] S. Aaronson, Certified randomness from quantum supremacy, Talk at CRYPTO 2018 (2018).
 - [33] R. Bassirian, A. Bouland, B. Fefferman, S. Gunn, and A. Tal, On certified randomness from quantum advantage experiments, arXiv preprint arXiv:2111.14846 (2021).
 - [34] S. Aaronson and S.-H. Hung, Certified randomness from quantum supremacy, arXiv preprint arXiv:2303.01625 (2023).
 - [35] A. Morningstar, M. Hauru, J. Beall, M. Ganahl, A. G. Lewis, V. Khemani, and G. Vidal, Simulation of quantum many-body dynamics with tensor processing units: Floquet prethermalization, *PRX Quantum* **3**, 020331 (2022).
 - [36] Z. Brakerski, P. Christiano, U. Mahadev, U. Vazirani, and T. Vidick, A cryptographic test of quantumness and certifiable randomness from a single quantum device, in *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, 2018) pp. 320–331.
 - [37] U. Mahadev, U. Vazirani, and T. Vidick, Efficient certifiable randomness from a single quantum device, arXiv preprint arXiv:2204.11353 (2022).
 - [38] M.-H. Yung and B. Cheng, Anti-forging quantum data: Cryptographic verification of quantum computational power, arXiv preprint arXiv:2005.01510 (2020).
 - [39] L. Brandão and R. Peralta, Notes on interrogating random quantum circuits, National Institute of Standards and Technology (2020), doi: 10.13140/RG.2.2.24562.94400.
 - [40] F. Pan and P. Zhang, Simulating the sycamore quantum supremacy circuits, arXiv preprint arXiv:2103.03074 (2021).
 - [41] S. P. Vadhan, Pseudorandomness, *Foundations and Trends in Theoretical Computer Science* **7**, 1 (2012).
 - [42] L. Trevisan, Extractors and pseudorandom generators, *Journal of the ACM* **48**, 860 (2001).
 - [43] R. Raz, O. Reingold, and S. Vadhan, Extracting all the randomness and reducing the error in Trevisan's extractors, *Journal of Computer and System Sciences* **65**, 97 (2002).
 - [44] W. Mauerer, C. Portmann, and V. B. Scholz, A modular framework for randomness extraction based on trevisan's construction, arXiv preprint arXiv:1212.0520 (2012).
 - [45] V. Shoup, Ntl: A library for doing number theory (2020).
 - [46] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction, *Physical Review A* **87**, 062327 (2013).
 - [47] National Institute of Standards and Technology, *FIPS PUB 198-1: The Keyed-Hash Message Authentication Code (HMAC)* (National Institute for Standards and Technology, 2008).
 - [48] Y. Dodis, R. Gennaro, J. Håstad, H. Krawczyk, and T. Rabin, Randomness extraction and key derivation using the cbc, cascade and hmac modes, in *Advances in Cryptology – CRYPTO 2004*, edited by M. Franklin (Springer Berlin Heidelberg, Berlin, Heidelberg, 2004) pp. 494–510.