QUANTUM INFORMATION

Random unitaries in extremely low depth

Thomas Schuster[1,2,3]*, Jonas Haferkamp[4,5]*, Hsin-Yuan Huang[3,2,6]*

Random unitaries are central to quantum technologies and the study of complex quantum many-body physics. However, existing protocols for generating random unitaries require long evolution times and deep circuits. In this work, we prove that local quantum circuits can form random unitaries in extremely low depth on any geometry. These shallow circuits have low complexity and create only short-range correlations, yet are indistinguishable from random unitaries with exponential complexity. This finding contrasts sharply with classical systems, in which a long evolution time is required to appear random. Our results have widespread applications across quantum science, from device benchmarking to quantum advantages. Moreover, they reveal that fundamental physical properties—including evolution time, causal structure, and phases of matter—are provably hard to learn.

Random processes are fundamental to both technology (*1*–*5*) and our understanding of nature (*6*–*8*). In quantum systems, the analog of a random process is a Haar-random unitary operation. Random unitaries form the backbone of numerous components of quantum technologies, including quantum device benchmarking (*9*–*11*), efficient measurement protocols (*12*–*14*), quantum advantage demonstrations (*15*–*18*), and quantum cryptography (*19*–*21*). They also serve as essential models for understanding quantum chaos (*22*–*24*), quantum machine learning (*25*–*27*), and quantum gravity (*28*, *29*).

A central open question concerns the minimal time, or circuit depth, needed for a local quantum circuit to behave like a Haar-random unitary. This determines both the resources required to implement such unitaries on a quantum device and their relevance as models of physical systems. Although a true Haar-random unitary requires exponential time to generate, two important approximations have emerged: approximate unitary k-designs (*30*–*33*), which mimic a Haar-random unitary U in any experiments using U up to k times, and pseudorandom unitaries (*19*, *34*, *35*), which mimic a Haar-random unitary in any efficient quantum experiments (Fig. 1). Enormous effort has gone into constructing these random unitaries in as low a depth as possible (*19*, *34*–*45*). Despite extensive research, all known constructions require circuit depths that grow polynomially with the qubit count n.

In this work, we show that local quantum circuits can form random unitaries in exponentially lower depths on any circuit geometry, including a one-dimensional (1D) line. Our construction glues together small random unitaries on local patches of $\log n$ or $\mathrm{poly}(\log n)$ qubits to create approximate designs or pseudorandom unitaries on n qubits (Fig. 2). By instantiating the small random unitaries with existing constructions (*34*, *35*, *43*, *45*), we achieve three main results: approximate unitary designs in $\log n$ depth on any circuit geometry, and pseudorandom unitaries in $\mathrm{poly}(\log n)$ depth on any geometry, and $\mathrm{poly}(\log\log n)$ depth in all-to-all-connected circuits. In all three cases, we prove that our achieved scaling in the system size n is optimal.

Our results reveal a sharp contrast with classical systems, in which a time/depth linear in the system size n is necessary to mimic truly random classical dynamics. The fact that quantum dynamics can become indistinguishable from random in exponentially shorter time than classical dynamics is surprising in many regards. Indeed, several extremely basic properties of physical systems, such as their causal structure and entanglement entropy, require at least linear depth to approach their truly random behaviors. If these properties were efficiently observable, they could be used to distinguish our constructed short-time random unitaries from exponential-time Haar-random unitaries. The resolution to this seeming contradiction is that our results prove that these basic physical properties are in fact not efficiently observable in any quantum experiment that can access the unitary U many times (*46*).

These discoveries have wide-ranging implications across quantum science. In classical shadow tomography (*12*, *47*–*49*), our approximate unitary designs enable estimation of highly nonlocal observables using log-depth instead of linear-depth circuits. This substantially reduces the experimental resources needed for classical shadows, making near-term implementations feasible for larger qubit counts. In many-body physics, our pseudorandom construction rigorously establishes that identifying topological order (*50*) is super-polynomially hard for any quantum experiment. Additional applications include quantum advantages for learning low-complexity dynamics and improved hardness results for random circuit sampling (*15*).

Low-depth random unitary designs

We now introduce our random circuit construction (Fig. 2) and present our main results. For simplicity, we begin with the simplest possible circuit geometry: a 1D line. We organize the n qubits of the 1D line into m local patches of $\xi = n/m$ qubits each. Our random unitary ensemble $\mathcal{E}$ corresponds to a two-layer circuit, in which small random unitaries act on pairs of neighboring patches in a brickwork fashion between the two layers. When these small random unitaries have depth d in terms of two-qubit gates, our proposed construction has total circuit depth $2d$.

We first show how our construction yields low-depth unitary designs. An ensemble $\mathcal{E}$ forms an ε-approximate unitary k-design if it approximates the Haar ensemble H up to error ε in any quantum experiment querying U up to k times. The gold standard for quantifying this approximation (*38*) is

$$(1-\varepsilon)\ \Phi_H \ \le\ \Phi_{\mathcal{E}} \ \le\ (1+\varepsilon)\ \Phi_H \tag{1}$$

where $\Phi_{\mathcal{E}}(\cdot) = \mathbb{E}_{U\sim\mathcal{E}}\left[U^{\otimes k}\cdot U^{\dagger,\otimes k}\right]$, and similarly for Φ_H. Here, $\Phi \le \Phi'$ denotes that $\Phi' - \Phi$ is completely positive. Physically, this inequality guarantees that the output state of any experiment involving U sampled from $\mathcal{E}$ up to k times is 2ε-close in trace distance to the output state when U is sampled from the Haar ensemble H.

Let us assume that each small random unitary in the two-layer brickwork ensemble $\mathcal{E}$ is drawn independently from an ε/n-approximate unitary k-design on 2ξ qubits. Our main result shows that the resulting ensemble $\mathcal{E}$ forms an ε-approximate unitary k-design whenever the number ξ of qubits in each local patch is at least logarithmic in n, k, and ε^{-1}.

Theorem 1 (Gluing small random unitary designs) For any approximation error $\varepsilon \le 1$, suppose each small random unitary in the two-layer brickwork ensemble $\mathcal{E}$ is drawn from an ε/n-approximate unitary k-design on 2ξ qubits with circuit depth d. Then $\mathcal{E}$ forms an ε-approximate unitary k-design on n qubits with depth $2d$, whenever the local patch size satisfies $\xi \ge \log_2\left(nk^2/\varepsilon\right)$.

[1]Walter Burke Institute for Theoretical Physics, California Institute of Technology, Pasadena, CA, USA. [2]Institute for Quantum Information and Matter, California Institute of Technology, Pasadena, CA, USA. [3]Google Quantum AI, Los Angeles, CA, USA. [4]Harvard John A. Paulson School Of Engineering And Applied Sciences, Cambridge, MA, USA. [5]Department of Mathematics, Saarland University, Saarbruecken, Germany. [6]Center for Theoretical Physics, Massachusetts Institute of Technology, Cambridge, MA, USA. ***Corresponding author. Email: schuster@caltech.edu (T.S.); jhaferkamp42@gmail.com (J.H.); hsinyuan@caltech.edu (H.-Y.H.)**

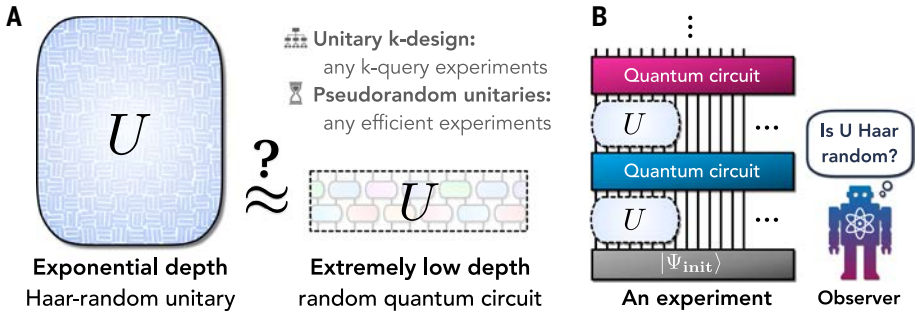

Fig. 1. Random unitaries and quantum experiments. The central question we seek to answer is: How shallow can a quantum circuit be while replicating the behavior of a Haar-random unitary? (**A**) A Haar-random unitary over n qubits requires a circuit depth that grows exponentially in n. Approximate unitary k-designs replicate the behavior of Haar-random unitaries within any quantum experiment that queries the unitary k times. Pseudorandom unitaries replicate the behavior of Haar-random unitaries within any efficient quantum experiment. (**B**) Any quantum experiment can be represented as follows: An observer prepares an initial state $|\Psi_{\text{init}}\rangle$, applies the unitary U many times, interleaved with many quantum circuits for quantum information processing, and concludes by performing a measurement (not shown).

Although several PRU constructions have been proposed (*19*, *34*, *35*, *42*, *43*), all known constructions require circuit depth poly(n). To construct PRUs in exponentially lower depths, we draw each small random unitary in our two-layer brickwork ensemble $\mathcal{E}$ from a PRU ensemble on 2ξ qubits, setting $\xi = \omega(\log n)$. We assume that each small unitary is secure against poly(n)-time quantum adversaries. Because $\xi = \omega(\log n)$, a poly(n)-time adversary is an $\exp(o(\xi))$-time adversary, which is automatically satisfied by using any PRU ensemble with subexponential security (*34*). Our main finding is that the resulting ensemble $\mathcal{E}$ forms an n-qubit PRU (*51*).

Theorem 2 (Gluing small pseudorandom unitaries) Suppose each small random unitary in the two-layer brickwork ensemble $\mathcal{E}$ is a 2ξ-qubit pseudorandom unitary secure against poly(n)-time adversaries for $\xi = \omega(\log n)$. Then $\mathcal{E}$ forms an n-qubit pseudorandom unitary secure against poly(n)-time adversaries.

The main ideas and technical lemmas behind the theorem are described in the materials and methods (*51*). Proof details are provided in the supplementary text section 3.3.

By using existing constructions of random unitary designs for the small random unitaries, Theorem 1 immediately yields designs in very low depth.

Corollary 1 (Low-depth random unitary designs) Random quantum circuits over n qubits can form ε-approximate unitary k-designs in circuit depth: $d = \mathcal{O}(\log(n/\varepsilon) \cdot k \,\text{poly}(\log k))$, for 1D circuits without ancilla qubits and $k \leq \Theta\left(2^{2n/5}\right)$, and $d = \mathcal{O}(\log\log(n/\varepsilon))$, for all-to-all circuits with $\mathcal{O}(n\log(n/\varepsilon))$ ancilla qubits and $k \leq 3$.

For general k, we take each small unitary to be a 1D local random circuit on 2ξ qubits, which forms an ε/n-approximate k-design in depth $d = \mathcal{O}((k\xi + \log(n/\varepsilon))\,\text{poly}(\log k))$ for $k \leq \Theta\left(2^{2(2\xi)/5}\right)$ (*45*, *52*). For $k \leq 3$, we use random Clifford unitaries (*53*), implementable in depth $d = \mathcal{O}(\log \xi)$ using ancilla qubits and nonlocal two-qubit gates (*54*). In both cases, our result exponentially improves the system size n dependence over all known constructions.

Finally, we prove that the system size n dependence of our approximate unitary designs is optimal for both 1D circuits and general all-to-all circuit architectures.

Proposition 1 (Depth lower bound for unitary designs) Consider any $k \geq 2$. A quantum circuit ensemble over n qubits that forms an approximate unitary k-design requires circuit depth: $d = \Omega(\log n)$, for 1D circuits with any number of ancilla qubits, and $d = \Omega(\log\log n)$, for all-to-all circuits with any number of ancilla qubits.

The proposition follows by analyzing the output distribution when a state $U|0^n\rangle$ is measured in a random product basis. When U is too shallow, the output distribution features large fluctuations in its low-weight marginals that differ from those of a Haar-random unitary (*51*). A lower bound proving the optimality of our ε dependence is in the supplementary text section 3.6.

Low-depth pseudorandom unitaries

We now show how our construction (Fig. 2) also yields low-depth pseudorandom unitaries (PRUs). PRUs are random unitary ensembles that are indistinguishable from the Haar ensemble by any efficient quantum algorithm that can query U many times (*19*, *42*, *43*). Specifically, an n-qubit PRU is secure against a $t(n)$-time adversary if it is indistinguishable from a Haar unitary by any $t(n)$-time quantum algorithm. An introduction to PRUs is in supplementary text section 4.

Using existing PRU constructions (*34*, *35*, *43*) to instantiate each small random unitary, which rely on the widely accepted conjecture regarding the quantum hardness of learning with errors (LWE) (*55*), we obtain n-qubit pseudorandom unitaries in the following low circuit depths.

Corollary 2 (Low-depth pseudorandom unitaries) Under the conjecture that no subexponential-time quantum algorithm can solve LWE, random quantum circuits over n qubits can form pseudorandom unitaries secure against any polynomial-time quantum adversary in circuit depth: $d = \text{poly}(\log n)$, for 1D circuits, and $d = \text{poly}(\log\log n)$, for all-to-all circuits.

Our depth improves exponentially over all known proposals (*19*, *34*, *35*, *42*, *43*), which require poly(n) depth for 1D circuits and poly(log n) depth for all-to-all circuits. Moreover, our scaling is optimal: Recent work shows that any 1D circuit of depth $\mathcal{O}(\log n)$ and any general circuit of depth $\mathcal{O}(\log\log n)$ can be learned in polynomial time (*56*), implying that 1D circuits require $\omega(\log n)$ depth and general circuits require $\omega(\log\log n)$ depth to form PRUs. These shallow quantum circuits have extremely low complexity and generate only short-range entanglement, yet they are indistinguishable from unitaries with exponential complexity. This result shows that the evolution time of a quantum system is not physically observable, even when considering the two extremes of poly(log n) and exp(n) time scales.

Comparison between quantum and classical circuits

It is instructive to contrast our results with random classical circuits. A simple light-cone argument (Fig. 3) shows that it easy to distinguish short-time from long-time classical dynamics, and hence classical circuits require depth $d = \Omega(n)$ in 1D and $d = \Omega(\log n)$ in all-to-all geometries to be indistinguishable from exponentially complex truly random dynamics. By contrast, quantum dynamics become indistinguishable from truly random dynamics in exponentially shorter time.

This exponential reduction is made possible by a fundamental feature of quantum mechanics: the abundance of noncommuting observables. To distinguish any circuit (classical or quantum) from a truly random one, an observer must eventually measure the system in some chosen basis. Noncommuting observables allow quantum circuits to locally hide information in observables unlikely to commute with any fixed basis. This causes measurement outcomes to be nearly independent of the random unitary's details, enabling it to appear exponentially complex at very low depths. We formalize this intuition in our

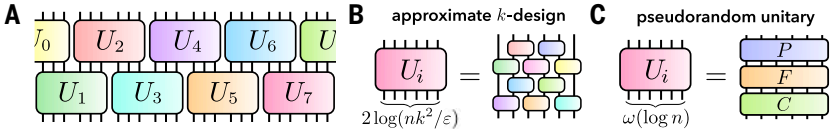

Fig. 2. Low-depth random unitary construction. (**A**) We consider a two-layer brickwork circuit, in which each small unitary acts on 2ξ qubits in each layer. (**B**) To generate ε-approximate unitary k-designs in $\log n$ depth, we draw each small unitary from an approximate unitary k-design on $2\xi = 2\log_2(nk^2/\varepsilon)$ qubits. (**C**) To generate pseudorandom unitaries in $\text{poly}(\log n)$ depth, we draw each small unitary from a pseudorandom unitary ensemble, such as the *PFC* ensemble (*34*,*35*,*43*), on $2\xi = \omega(\log n)$ qubits.

proof of the lower bound on unitary designs in the materials and methods (*51*).

Creating random unitaries on any geometry

We provide two methods to extend our construction from 1D circuits to any circuit geometry. Our first method shows that any depth-d quantum circuit on a 1D line can be implemented on any geometry in depth $\mathcal{O}(d)$. The key is to efficiently construct a path on the geometry that visits every qubit exactly once. Although such paths do not always exist and are generally hard to find, we prove that allowing jumps to constant-distance neighbors guarantees the existence of an efficiently constructible path (Fig. 3B). Two-qubit gates between constant-distance neighbors can then be implemented using a carefully designed swap network. Our second method extends Theorem 1 directly to general two-layer brickwork circuits. This enables gluing together small random unitaries on various geometries of interest, such as a 2D circuit consisting of overlapping squares (fig. S1C). Both methods apply to both our constructions of low-depth unitary designs and low-depth PRUs. Details are in supplementary text section 5.

Applications

We now present key applications of our results (Fig. 4), with full details in supplementary text section 6.

Provably efficient shallow classical shadows

Classical shadows use random measurements to estimate many noncommuting observables (*12*). Standard shadow protocols require random Clifford unitaries, with linear circuit depth. We prove these can be replaced by log n-depth Clifford circuits from our construction while maintaining the same sample complexity guarantees, confirming conjectures in (*47*, *48*). A key motivation for these shallow shadow protocols is to address experimental limitations on circuit depths due to noise in quantum devices. Given any linear-depth circuit compilation of random Clifford circuits, our construction can achieve a provable 2 to 3 times reduction in circuit depth for $n = 100$ qubits and a 100 times depth reduction for $n = 6000$ qubits.

Quantum hardness of recognizing topological order

The detection of topologically ordered phases of matter has remained a notoriously difficult challenge across both materials and atomic, molecular, and optical experiments (*50*, *57*, *58*). A defining feature of topological order is its invariance under low-depth local unitary circuits (*50*). Using Corollary 2, we prove:

Corollary 3 (Hardness of recognizing topological order) For any definition of topological order where (i) the product state has trivial order and the toric code state has nontrivial order, and (ii) this order is preserved under any depth-ℓ geometrically local circuit, recognizing topological order is quantum computationally hard for any $\ell = \Omega(\text{polylog } n)$.

The criteria in the corollary apply to nearly all existing definitions of topological order (*59*).

Quantum advantage for learning low-complexity quantum systems

Several well-known quantum learning advantages (*60*–*63*) have so far applied only to highly complex systems. For instance, distinguishing a random unitary from a depolarizing channel requires superpolynomial time for classical observers but is easy for quantum observers (*62*, *63*). Until now, this advantage was only known for Haar-random unitaries, which require $\exp(\mathcal{O}(n))$ time to generate and are thus poor models for physical processes. Our results show that this superpolynomial advantage holds for dynamics of double-exponentially shorter time, $\text{poly}(\log n)$. We also establish similar quantum-classical separations for learning entanglement structure in short-range entangled states.

The power of time-reversal for learning causal structures

Leveraging interaction engineering techniques, some modern quantum experiments have the ability to time-reverse their dynamics (*64*–*66*). A surprising consequence of our results is that such experiments can learn properties of quantum dynamics exponentially more efficiently than standard experiments lacking time reversal (*67*, *68*). This advantage is particularly pronounced for uncovering the causal structure of the dynamics. For example, our results show that detecting whether a shallow circuit contains only local interactions versus a mix of local and long-range couplings is hard without time reversal, but becomes easy with it; see supplementary text section 6.4. This separation is fundamentally quantum mechanical, following light-cone arguments similar to those in Fig. 3A.

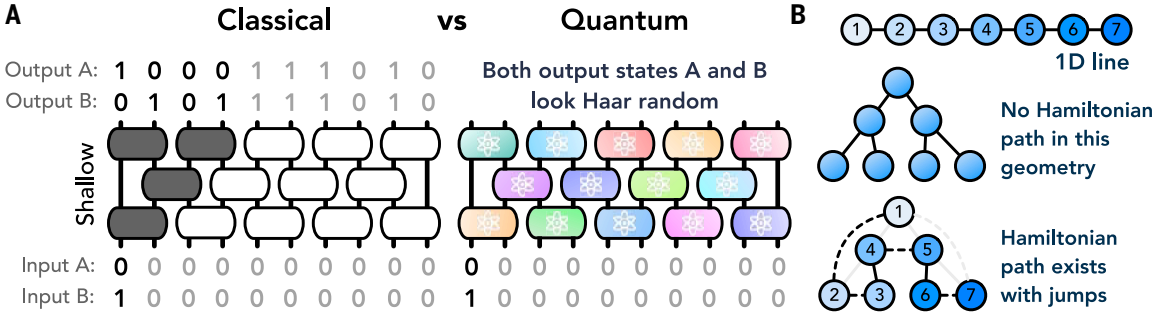

Fig. 3. Comparison with classical circuits, and extension to any circuit geometry. (**A**) Shallow random classical circuits cannot look uniformly random. By contrast, our results show that shallow random quantum circuits can already look Haar-random. (**B**) To create random unitaries on any circuit geometry, we implement a 1D random circuit along a Hamiltonian path of the geometry. Although Hamiltonian paths do not exist in any geometry, when jumping to constant-distance neighbor is allowed, they always exist and are efficient to construct.

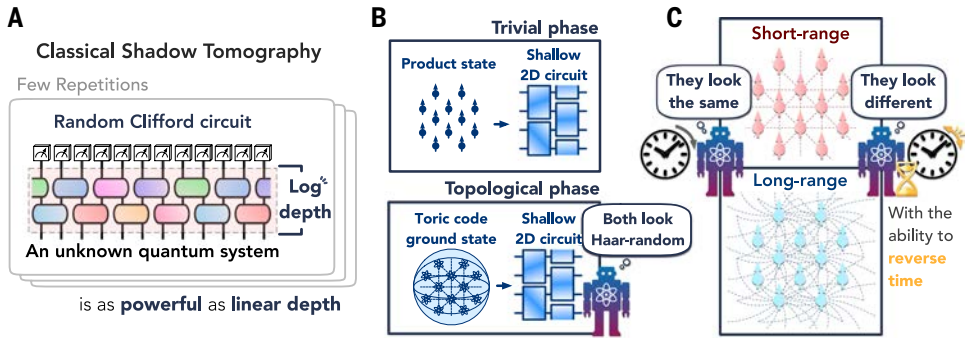

Fig. 4. Applications of low-depth random unitaries. (**A**) Log-depth classical shadows: Our shallow unitary 3-designs enable provably efficient classical shadow tomography using $\log(n)$-depth random Clifford circuits instead of linear depth. (**B**) Quantum hardness of recognizing topological order: By applying our shallow pseudorandom unitaries to product and toric code states, we generate pseudorandom states with trivial and topological order, respectively. This demonstrates that recognizing topological order in an unknown state is quantumly hard. (**C**) Power of time-reversal in learning: We establish that quantum experiments capable of reversing time evolution can exhibit superpolynomial advantages over conventional experiments. We prove this in a simple example where one wishes to detect whether long-range couplings are present in a strongly interacting dynamical quantum system.

Output distributions of random quantum circuits

Random circuit sampling (RCS) is a leading candidate for quantum computational advantage (*15*). Proofs of its hardness require both worst-case hardness and anti-concentration (*16*, *17*)—requirements previously met only in 2D circuits of depth $\Omega(\sqrt{n})$ (*40*). Our approximate unitary 2-designs achieve both properties in depth $\log n$. Furthermore, using higher-k designs, we prove that at depth $\Omega(\log n)$, the output distributions of random circuits are far from uniform with probability close to one, and at depth $\mathrm{poly}(\log n)$, they become computationally indistinguishable from uniform while remaining far from it.

Barren plateaus in variational quantum algorithms

Variational quantum algorithms represent a promising approach for quantum computing applications (*27*). However, these algorithms encounter optimization challenges known as barren plateaus, which arise when the parameterized quantum circuits approach unitary 2-designs under random initialization, leading to vanishingly small loss function variances (*25*). As an ε-approximate unitary 2-design yields a loss function variance of $\mathcal{O}\left(\varepsilon+\frac{1}{2^n}\right)$, our results imply that barren plateaus with loss function variance ϵ emerge at circuit depths of only $\mathcal{O}(\log(n/\epsilon))$ for both local and global observables. This scaling reveals that circuits with depth slightly higher than logarithmic, e.g., $d=\Omega\left(\log(n)^2\right)$, inevitably produce barren plateaus with variance smaller than any $1/\mathrm{poly}(n)$, creating insurmountable optimization barriers even for shallow quantum circuits with local cost functions (*69*). These results underscore the need for structured, problem-specific ansätze for practical applications.

Discussion

We have shown that random unitaries can be naturally generated in extremely low circuit depths. Our results reveal a surprising and profound property of quantum circuits that differs fundamentally from those of classical systems. Our construction of random unitaries is both exceptionally simple and highly versatile, offering benefits from both experimental and theoretical perspectives.

These discoveries open numerous avenues for future research. The applications that we have explored likely represent only a fraction of the potential impact, given that random unitaries are ubiquitous tools in quantum technology and in understanding complex quantum processes. In quantum benchmarking, efficient learning using random unitaries extends to fermionic, bosonic, and Hamiltonian systems (*13*, *24*, *70*–*72*). Can one show that the formation of random unitaries in extremely short times applies to these systems as well? In quantum gravity, a widespread conjecture states that black holes are the fastest scramblers in nature (*28*). If we consider scrambling to be the formation of random unitary designs, could our discovery of surprisingly fast design formation on any geometry provide new insight into quantum black holes and the holographic correspondence (*73*, *74*)?

Perhaps most intriguingly, the ability to generate random unitaries in extremely low depth reveals fundamental limits on what is physically observable. Our results show that several fundamental physical properties—evolution time, phases of matter, and causal structure—are provably hard to learn through conventional quantum experiments. This raises profound questions about the nature of physical observation itself: What other fundamental physical properties might be intrinsically hard to measure? What are the implications of these properties being imperceptible? Should physical theories contain quantities that are fundamentally hard to see, or does this suggest a deeper principle about the nature of physical reality?

REFERENCES AND NOTES

1. M. Blum, S. Micali, *SIAM J. Comput.* **13**, 850–864 (1984).
2. L. Blum, M. Blum, M. Shub, *SIAM J. Comput.* **15**, 364–383 (1986).
3. Reuven Y Rubinstein and Dirk P Kroese, *Simulation and the Monte Carlo method* (John Wiley & Sons, 2016).
4. M. Santha, U. V. Vazirani, *J. Comput. Syst. Sci.* **33**, 75–87 (1986).
5. J. Håstad, R. Impagliazzo, L. A. LevinM. Luby, *SIAM J. Comput.* **28**, 1364–1396 (1999).
6. A. Einstein, *Ann. Phys.* **322**, 549–560 (1905).
7. J. S. Linda, *Allen. An Introduction to Stochastic Processes with Applications to Biology* (CRC Press, 2010).
8. E. P. Wigner, *SIAM Rev.* **9**, 1–23 (1967).
9. J. Emerson, R. Alicki, K. Życzkowski, *J. Opt. B Quantum Semiclassical Opt.* **7**, S347–S352 (2005).
10. E. Knill *et al.*, *Phys. Rev. A* **77**, 012307 (2008).
11. A. Elben *et al.*, *Phys. Rev. Lett.* **125**, 200501 (2020).
12. H.-Y. Huang, R. Kueng, J. Preskill, *Nat. Phys.* **16**, 1050–1057 (2020).
13. A. Zhao, N. C. Rubin, A. Miyake, *Phys. Rev. Lett.* **127**, 110504 (2021).
14. A. Elben *et al.*, *Nat. Rev. Phys.* **5**, 9–24 (2023).
15. F. Arute *et al.*, *Nature* **574**, 505–510 (2019).
16. R. Movassagh, *Nat. Phys.* **19**, 1719–1724 (2023).
17. A. Bouland, B. Fefferman, C. Nirkhe, U. Vazirani, *Nat. Phys.* **15**, 159–163 (2019).
18. A. Morvan *et al.*, Phase transition in random circuit sampling. arXiv:2304.11119 [quant-ph] (2023).
19. Z. Ji, Y.-K. Liu, F. Song, Pseudorandom quantum states, in *Advances in Cryptology–CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part III* (Springer, 2018), pp. 126–152.
20. P. Ananth, L. Qian, H. Yuen, Cryptography from pseudorandom quantum states, in *Annual International Cryptology Conference* (Springer, 2022), pp. 208–236.
21. W. Kretschmer, L. Qian, M. Sinha, A. Tal, Quantum cryptography in algorithmica" in *Proceedings of the 55th Annual ACM Symposium on Theory of Computing* (2023), pp. 1589–1602.
22. A. Nahum, J. Ruhman, S. Vijay, J. Haah, *Phys. Rev. X* **7**, 031016 (2017).
23. A. Nahum, S. Vijay, J. Haah, *Phys. Rev. X* **8**, 021014 (2018).
24. J. Choi *et al.*, *Nature* **613**, 468–473 (2023).
25. J. R. McClean, S. Boixo, V. N. Smelyanskiy, R. Babbush, H. Neven, *Nat. Commun.* **9**, 4812 (2018).
26. E. R. Anschuetz, B. T. Kiani, *Nat. Commun.* **13**, 7760 (2022).
27. M. Larocca *et al.*, arXiv:2405.00781 [quant-ph] (2024).
28. Y. Sekino,L. Susskind, *J. High Energy Phys.* **2008**, 065 (2008).
29. P. Hayden, J. Preskill, *J. High Energy Phys.* **2007**, 120 (2007).
30. J. Emerson, Y. S. Weinstein, M. Saraceno, S. Lloyd, D. G. Cory, *Science* **302**, 2098–2100 (2003).

31. D. Gross, K. Audenaert, J. Eisert, *J. Math. Phys.* **48**, 052104 (2007).
32. C. Dankert, arXiv:quant-ph/0512217 [quant-ph] (2005).
33. C. Dankert, R. Cleve, J. Emerson, E. Livine, *Phys. Rev. A* **80**, 012304 (2009).
34. F. Ma, H.-Y. Huang, arXiv:2410.10116 [quant-ph] (2024).
35. A preliminary note for constructing n-qubit polylog(n)-depth pseudorandom unitaries secure against $exp(o(n))$-time adversary can be found at https://hsinyuan-huang.github.io/assets/img/FermiMa_HsinYuanHuang_PolyLogDepthPRUs_against_SubExpAdv.pdf.
36. J. Emerson, E. Livine, S. Lloyd, *Phys. Rev. A* **72**, 060302 (2005).
37. A. W. Harrow, R. A. Low; Aram W Harrow and Richard A Low, *Commun. Math. Phys.* **291**, 257–302 (2009).
38. G. S. L. Fernando, Horodecki. Local random quantum circuits are approximate polynomial-designs. *Commun. Math. Phys.* **346**, 397–434 (2016).
39. J. Haferkamp, *Quantum* **6**, 795 (2022).
40. A. W. Harrow, S. Mehraban, *Commun. Math. Phys.* **401**, 1531–1626 (2023).
41. S.-K. Jian, G. Bentsen, B. Swingle, *J. High Energy Phys.* **2023**, 190 (2023).
42. C.-F. Chen, A. Bouland, F. G. S. L. Brandão, J. Docter, P. Hayden, M. Xu, Efficient unitary designs and pseudorandom unitaries from permutations. arXiv:2404.16751 [quant-ph] (2024).
43. T. Metger, A. Poremba, M. Sinha, H. Yuen, arXiv:2404.12647 [quant-ph] (2024). https://doi.org/10.1109/FOCS61266.2024.00038
44. J. Haah, Y. Liu, X. Tan, arXiv:2402.05239 [quant-ph] (2024). https://doi.org/10.1109/FOCS61266.2024.00036
45. C.-F. Chen *et al.*, arXiv:2406.07478 [quant-ph] (2024).
46. Intriguingly, this essential point does not carry over to experiments that query both the unitary U and its inverse, $U^{\dagger}$ (*67*, *68*). See the applications section and Appendix 6.4 for further discussions.
47. C. Bertoni *et al.*, arXiv:2209.12924 [quant-ph] (2022).
48. M. Ippoliti, Y. Li, T. Rakovszky, V. Khemani, *Phys. Rev. Lett.* **130**, 230403 (2023).
49. H.-Y. Hu, S. Choi, Y.-Z. You, *Phys. Rev. Res.* **5**, 023027 (2023).
50. X.-G. Wen, *Rev. Mod. Phys.* **89**, 041004 (2017).
51. Materials and methods are available as supplementary materials.
52. This k dependence is optimal up to poly(log k) factors (*45*). Hence, our k dependence is similarly optimal.
53. Z. Webb, arXiv:1510.02769 [quant-ph] (2015).
54. J. Jiang *et al.*, Optimal space-depth trade-off of cnot circuits in quantum logic synthesis" in *Proceedings of the Fourteenth Annual ACM-SIAM Symposium on Discrete Algorithms* (SIAM, 2020), pp. 213–229.
55. O. Regev, *J. Assoc. Comput. Mach.* **56**, 1–40 (2009) (JACM).
56. H.-Y. Huang *et al.*, Jarrod R McClean, "Learning shallow quantum circuitsin *Proceedings of the 56th Annual ACM Symposium on Theory of Computing* (2024), pp. 1343–1351.
57. G. Semeghini *et al.*, *Science* **374**, 1242–1247 (2021).
58. J. Léonard *et al.*, *Nature* **619**, 495–499 (2023).
59. Definitions of topological order are often stated colloquially in terms of constant-depth circuits, i.e., $= \mathcal{O}(1)$. However, more precise definitions are nearly always robust up to any depth that is subextensive in the system diameter, e.g., $= o\left(\sqrt{n}\right)$ in 2D. We refer to Appendix 6.2 for a detailed discussion.
60. D. Aharonov, J. Cotler, X.-L. Qi, *Nat. Commun.* **13**, 887 (2022).
61. H.-Y. Huang, R. Kueng, J. Preskill, *Phys. Rev. Lett.* **126**, 190505 (2021).
62. H.-Y. Huang *et al.*, *Science* **376**, 1182–1186 (2022).
63. S. Chen, J. Cotler, H.-Y. Huang, J. Li, "Exponential separations between learning with and without quantum memory" in *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, 2022), pp. 574–585.
64. J. Baum, M. Munowitz, A. N. Garroway, A. Pines, *J. Chem. Phys.* **83**, 2015–2025 (1985).
65. S. Choi, N. Y. Yao, M. D. Lukin, *Phys. Rev. Lett.* **119**, 183603 (2017).
66. M. Gärttner *et al.*, *Nat. Phys.* **13**, 781–786 (2017).
67. J. Cotler, T. Schuster, M. Mohseni, *Phys. Rev. A* **108**, 062608 (2023).
68. T. Schuster *et al.*, *Phys. Rev. Res.* **5**, 043284 (2023).
69. M. Cerezo, A. Sone, T. Volkoff, L. Cincio, P. J. Coles, *Nat. Commun.* **12**, 1791 (2021).
70. K. Wan, W. J. Huggins, J. Lee, R. Babbush*Commun. Math. Phys.* **404**, 629–700 (2023).
71. S. Gandhari, V. V. Albert, T. Gerrits, J. M. Taylor, M. J. Gullans, *PRX Quantum* **5**, 010346 (2024).
72. S. Becker, N. Datta, L. Lami, C. Rouzé, *IEEE Trans. Inf. Theory* **70**, 3427–3452 (2024).
73. J. Maldacena, *Int. J. Theor. Phys.* **38**, 1113–1133 (1999).
74. A. Bouland, B. Fefferman, U. Vazirani, arXiv:1910.14646 [quant-ph] (2019).

ACKNOWLEDGMENTS

We are grateful to E. Anschuetz, R. Babbush, C. Bertoni, A. Bouland, S. Boixo, F. Brandão, X. Chen, S. Choi, J. Cotler, J. Eisert, B. Fefferman, D. Gosset, S. Goush, P. Hayden, N. Hunter-Jones, M. Ioannou, M. Ippoliti, V. Khemani, I. Kim, W. Kretschmer, D. Kufel, D. Liang, F. Ma, J. R. McClean, T. Metger, R. Movassagh, Q. Nguyen, M. Soleimanifar, N. Tantivasadakarn, M. Tomamichel, U. Vazirani, and N. Yao for valuable discussions and insights. We thank S. Choi for introducing T.S. and J.H. to each other, which was vital for this work. **Funding:** T.S. acknowledges support from the Walter Burke Institute for Theoretical Physics at Caltech. J.H. acknowledges funding from the Harvard Quantum Initiative. H.H. acknowledges the visiting associate position at the Massachusetts Institute of Technology. T.S. and H.H. acknowledges support from the US Department of Energy, Office of Science, National Quantum Information Science Research Centers, Quantum Systems Accelerator. The Institute for Quantum Information and Matter, with which T.S. and H.H. are affiliated, is an NSF Physics Frontiers Center (NSF grant PHY-2317110). This work was conducted while J.H. and H.H. were at the Simons Institute for the Theory of Computing, supported by DOE QSA grant FP00010905. **Author contributions:** T.S. and J.H. independently conceived of the low-depth construction of unitary designs. T.S. and H.H. conceived of the low-depth construction of pseudorandom unitaries. All authors contributed to the theoretical development, proofs, applications, writing, and presentation of the work. **Competing interests:** There are no competing interests to declare. **Data and materials availability:** All data needed to evaluate the conclusions in the paper are present in the paper or the supplementary materials.

SUPPLEMENTARY MATERIALS

science.org/doi/10.1126/science.adv8590
Materials and Methods; Supplementary Text; Figs. S1 to S3; References (*75*–*157*)
Submitted 9 January 2025; accepted 13 May 2025
10.1126/science.adv8590