Efficient Quantum Pseudorandomness with Nearly Time-Independent Hamiltonian Dynamics

Yoshifumi Nakata,[1,2] Christoph Hirche,[2] Masato Koashi,[1] and Andreas Winter[2,3]
[1]*Photon Science Center, Graduate School of Engineering, The University of Tokyo, Bunkyo-ku, Tokyo 113-8656, Japan*
[2]*Departament de Física, Grup d'Informació Quàntica, Universitat Autònoma de Barcelona, ES-08193 Bellaterra (Barcelona), Spain*
[3]*ICREA: Institució Catalana de Recerca i Estudis Avançats, ES-08010 Barcelona, Spain*
(Received 7 November 2016; revised manuscript received 3 February 2017; published 10 April 2017)

Quantum randomness is an essential key to understanding the dynamics of complex many-body systems and also a powerful tool for quantum engineering. However, exact realizations of quantum randomness take an extremely long time and are infeasible in many-body systems, leading to the notion of quantum pseudorandomness, also known as unitary designs. Here, to explore microscopic dynamics of generating quantum pseudorandomness in many-body systems, we provide new efficient constructions of unitary designs and propose a design Hamiltonian, a random Hamiltonian of which dynamics always forms a unitary design after a threshold time. The new constructions are based on the alternate applications of random potentials in the generalized position and momentum spaces, and we provide explicit quantum circuits generating quantum pseudorandomness significantly more efficient than previous ones. We then provide a design Hamiltonian in disordered systems with periodically changing spin-glass-type interactions. The design Hamiltonian generates quantum pseudorandomness in a constant time even in the system composed of a large number of spins. We also point out the close relationship between the design Hamiltonian and quantum chaos.

DOI: 10.1103/PhysRevX.7.021006

Subject Areas: Quantum Physics, Quantum Information, Statistical Physics

I. INTRODUCTION

Random quantum process is a useful resource in quantum information processing, as one of the fundamental primitives in quantum Shannon theory [1–8] and to demonstrate quantum advantages in many protocols [9–18]. In recent years, random processes have also turned out to play key roles in understanding fundamental physics in complex quantum systems, leading to new developments in quantum thermodynamics [19–21] (see Ref. [22] for a comprehensive review), black hole information science [23–28], and strongly correlated many-body physics [29–31]. Quantum randomness is often represented by random unitaries drawn uniformly at random according to the Haar measure, referred to as Haar random unitaries. However, when a system is large, it takes an extremely long time to realize Haar random unitaries, implying that they rarely appear in natural systems composed of many particles. This is especially the case when the interactions are local. This fact has led to the research area on quantum pseudorandomness [32–35], particularly in terms of unitary t-designs [36–38], and their efficient implementations [33–35,39–47]. A unitary t-design is a finite-degree approximation of Haar random unitaries, and is called exact when it simulates all the first t moments of Haar random unitaries and approximate when the simulations are with errors.

Traditionally, unitary t-designs have been investigated for small t. In particular, unitary 2-designs were intensely studied [34,36–42,44,45] due to the fact that they are useful in important tasks, such as decoupling [5–8] and randomized benchmarking [9–12], and that the Clifford group is an exact unitary 2-design [36]. Unitary 2-designs have already been implemented experimentally in small systems and are a standard tool of evaluating the performance of quantum devices [48–51]. Later, the Clifford group on two-level systems, known as qubits, was also shown to be a unitary 3-design but not to be a 4-design [46,47,52]. For $t \geq 4$, a few applications are known (e.g., state discrimination [13], quantum speed-ups in query complexity [14], and compressed sensing [15,17]), but they are of potential importance when strong large deviation bounds are needed, which typically leads to better performance of quantum protocols. So far, only a couple of efficient implementations for $t \geq 4$ are known, to the best of our knowledge. One is to use a classical tensor product expander and the Fourier transformation, forming approximate unitary t-designs for $t = O(N/\log N)$ by using $\mathrm{poly}(N)$ quantum

gates [33]. The other is to use local random quantum circuits composed of random two-qubit gates applied onto neighboring qubits, which achieves approximate unitary t-designs for $t = \mathrm{poly}(N)$ using $O(t^{10}N^2)$ gates [35,43].

Despite these implementations of unitary designs by quantum circuits, there exists a certain gap between the constructions and physically feasible dynamics in quantum many-body systems. The constructions require a finely structured circuit [33] or the use of randomly varying interactions [35,43], while dynamics in physically feasible many-body systems is typically not structured and is generated by a Hamiltonian, which may slightly fluctuate over time but should be based on a time-independent one. Indeed, if we interpret local random quantum circuits on N qubits in terms of Hamiltonian dynamics, the interactions should be changed uniformly at random $O(t^{10}N)$ times before the dynamics achieves unitary t-designs. Because of its dependence on the number of qubits, the total Hamiltonian should be highly time dependent and may not be so physically feasible in large systems, resulting in the lack of a solid basis of a number of studies in many-body systems based on quantum pseudorandomness [19–28]. There is also an increasing demand from black hole information science and quantum chaos to fully understand microscopic dynamics of randomization, where so-called scrambling has been intensely studied [23–31]. Scrambling is a weak variant of quantum pseudorandomness, and studying natural Hamiltonians generating unitary designs will elaborate the understandings in context. Furthermore, implementations of unitary designs by Hamiltonian dynamics are of practical importance, helping experimental realizations of designs, as any quantum circuit is fundamentally implemented by engineering Hamiltonians.

In this paper, to better understand microscopic dynamics generating quantum pseudorandomness, we provide new constructions of unitary t-designs and propose a design Hamiltonian, a random Hamiltonian of which dynamics forms a unitary design at any time after a threshold time. The constructions are based on the scheme of repeating random unitaries diagonal in mutually unbiased bases [45,53–55]. We first show that the process on a d-dimensional Hilbert space, known as a qudit, achieves unitary t-designs after $O(t)$ repetitions if a pair of the two bases satisfies a certain condition, which is considered to be a generalization of the position and momentum bases. As the construction works for any space, it will be useful to implement unitary designs in a subspace, such as a bosonic subspace, which is a strong resource to demonstrate a quantum advantage in metrology [18]. We then focus on random diagonal unitaries in the Pauli-X and -Z bases on N qubits and investigate how to approximate them efficiently by quantum circuits. By mapping this problem to a combinatorial problem, called a local permutation check problem, we show that an approximate unitary t-design for $t = o(N^{1/2})$ can be achieved by using $O(tN^2)$ gates. In terms of t, this drastically improves the previous result [35,43], which uses $O(t^{10}N^2)$ gates, and is essentially optimal. As higher designs are useful to improve the performance of any applications of lower designs due to their large deviation bounds [56], this construction will contribute to improving the performance of any applications of designs [1–18]. Finally, we present a nearly time-independent design Hamiltonian with spin-glass-type interactions, where it suffices to vary the interactions only $O(t)$ times before the corresponding time-evolution operators form unitary t-designs. As a consequence, the design Hamiltonians saturate expectation values of any observables, e.g., the so-called out-of-time-ordered (OTO) correlators [29–31], to the fully uniform averages in a constant time. As the saturation of OTO correlators is expected to be a sign of quantum chaos [28], this shows a close relation between design Hamiltonians and quantum chaos, further suggesting the possibility to explore fascinating features of random dynamics in complex quantum systems by design Hamiltonians and by the methods developed in quantum information science. We also propose a conjecture about the time scale for a natural design Hamiltonian to generate unitary designs, which can be seen as a generalization of the fast scrambling conjecture [24].

This paper is organised as follows. In Sec. II, we introduce necessary notations and explain several definitions and properties of random unitaries. All of the main results are summarized in Sec. III, of which proofs are provided in Sec. IV. We conclude and discuss possible future directions in Sec. V. Small propositions presented in the paper are explained in Appendixes.

II. PRELIMINARIES

We use the following standard asymptotic notation. Let $f(n)$ and $g(n)$ be functions on $\mathbb{R}^+$. We say $f(n) = O(g(n))$ if there exist c, $n_0 > 0$ such that $f(n) \le cg(n)$ for all $n \ge n_0$. When there exist c, $n_0 > 0$ such that $f(n) \ge cg(n)$ for all $n \ge n_0$, we say $f(n) = \Omega(g(n))$. If $f(n) = O(g(n))$ and $f(n) = \Omega(g(n))$, we denote it by $f(n) = \Theta(g(n))$. If $\lim_{n\to\infty} f(n)/g(n) = 0$, we write it by $f(n) = o(g(n))$. For given i, j ($i < j$), we denote by $[i, j]$ a sequence of numbers from i to j, $[i, j] := \{i, i+1, \ldots, j-1, j\}$. We also use a floor function $\lfloor x \rfloor$ for $x \in \mathbb{R}$, which is the largest integer less than or equal to x.

Let $\mathcal{H}$ be a Hilbert space and $\mathcal{B}(\mathcal{H})$ be a set of bounded operators on $\mathcal{H}$. We use several norms of operators and superoperators. For operators, we use the operator norm $\|\cdot\|_\infty$ and the p-norm ($p \ge 1$) defined by $\|X\|_\infty := \max_i x_i$, where $\{x_i\}$ are the singular values of X, and $\|X\|_p := (\mathrm{tr}|X|^p)^{1/p}$, respectively. For a superoperator $\mathcal{C}: \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$, we use a family of superoperator norms $\|\mathcal{C}\|_{q\to p}$ (q, $p \ge 1$) and the diamond norm [57] defined by

$$\|\mathcal{C}\|_{q\to p} = \sup_{X\neq 0} \frac{\|\mathcal{C}(X)\|_p}{\|X\|_q}, \qquad \|\mathcal{C}\|_\diamond := \sup_k \|\mathcal{C}\otimes \mathrm{id}_k\|_{1\to 1}, \quad (1)$$

respectively, where id_k is the identity map acting on a Hilbert space of dimension k.

Perfect quantum randomness is often represented by a Haar random unitary, a unitary drawn from a unitary group uniformly at random. Formally, it is given as follows: let $\mathcal{U}(d)$ be a unitary group of degree d, and H be the Haar measure (i.e., the unique unitarily invariant probability measure) on $\mathcal{U}(d)$. A Haar random unitary U^H is a $\mathcal{U}(d)$-valued random variable distributed according to the Haar measure, $U^H \sim \mathsf{H}$. Quantum randomness is hard to generate when the dimension of the unitary group is large due to its full uniformity. Moreover, when we consider the generation of quantum randomness in isolated physical systems, Haar random unitaries are extremely rare to appear because the dynamics in a physical system is generated by a system Hamiltonian and, if it is time independent, the dynamics leaves the eigenspaces invariant. In such situations, it may be more physically feasible to fix the basis and to consider random time evolution under the fixed basis. This is the idea of a random diagonal unitary [58] in a fixed basis: let $E = \{|k\rangle\}_{k\in[0,d-1]}$ be an orthogonal basis in a Hilbert space $\mathcal{H}$ with dimension d. Let $\mathcal{D}_E(d)$ be the set of $d \times d$ unitaries diagonal in the basis E. Let D_E denote a probability measure on $\mathcal{D}_E(d)$ induced by a uniform probability measure on the parameter space $[0, 2\pi)^d$. A random diagonal unitary in the basis of E [53], D^E, is a $\mathcal{D}_E(d)$-valued random variable distributed according to D_E, $D^E \sim \mathsf{D}_E$.

In practice, quantum randomness described by Haar random unitaries should be considered to be an idealization because the time necessary for exactly generating quantum randomness scales exponentially in the number of particles in the system. Hence, it is important to consider quantum pseudorandomness often described by a unitary t-design ($t \in \mathbb{Z}^+$). To explain unitary designs, let $\mathcal{G}^{(t)}_{U\sim\nu}(X)$ be a superoperator given by $\mathcal{G}^{(t)}_{U\sim\nu}(X) \coloneqq \mathbb{E}_{U\sim\nu}[U^{\otimes t} X U^{\dagger\otimes t}]$ for any $X \in \mathcal{B}(\mathcal{H}^{\otimes t})$, where $\mathbb{E}_{U\sim\nu}$ represents an average over a random unitary U according to a probability measure ν. Then, a random unitary $U \sim \nu$ is called an ϵ-approximate unitary t-design [34,37] if $\|\mathcal{G}^{(t)}_{U\sim\nu} - \mathcal{G}^{(t)}_{U\sim\mathsf{H}}\|_\diamond \le \epsilon$. Quantum pseudorandomness, in the sense of unitary t-designs, is indistinguishable from a fully random one even if we have t copies of the system and are allowed to collectively act on the whole of them. Hence, it is regarded as a lower-order approximation of quantum randomness.

Note that, if U is an ϵ-approximate unitary t-design, then for any random unitary V independent of U, UV and VU are also ϵ-approximate unitary t-designs. This can be seen in a straightforward way as follows:

$$\|\mathcal{G}^{(t)}_V \circ \mathcal{G}^{(t)}_{U\sim\nu} - \mathcal{G}^{(t)}_{U\sim\mathsf{H}}\|_\diamond = \|\mathcal{G}^{(t)}_V \circ (\mathcal{G}^{(t)}_{U\sim\nu} - \mathcal{G}^{(t)}_{U\sim\mathsf{H}})\|_\diamond \quad (2)$$

$$\le \|\mathcal{G}^{(t)}_V\|_\diamond \|\mathcal{G}^{(t)}_{U\sim\nu} - \mathcal{G}^{(t)}_{U\sim\mathsf{H}}\|_\diamond \quad (3)$$

$$\le \epsilon, \quad (4)$$

where we use the unitary invariance of the Haar measure in the first line, and a fact that $\mathcal{G}^{(t)}_V$ is a completely positive and trace-preserving map in the last line. The proof for UV is also similar.

We also use a quantum (η,t)-tensor product expander ν (TPE), which is considered to be a "seed" of quantum pseudorandomness, defined by

$$\|\mathbb{E}_{U\sim\nu}[U^{\otimes t,t}] - \mathbb{E}_{U\sim\mathsf{H}}[U^{\otimes t,t}]\|_\infty \le \eta, \quad (5)$$

where $\eta < 1$, $U^{\otimes t,t} \coloneqq U^{\otimes t} \otimes U^{*\otimes t}$, and U^* is a complex conjugation of U [59]. This definition is equivalent to

$$\|\mathcal{G}^{(t)}_{U\sim\nu} - \mathcal{G}^{(t)}_{U\sim\mathsf{H}}\|_{2\to2} \le \eta, \quad (6)$$

and, hence, the difference between a quantum TPE and a unitary t-design is just the norm used in their definitions. The quantum TPE is useful simply because iterating quantum (η, t) TPE yields an approximate unitary t-design. This fact is often used in the literature [33,35,43], which is stated in the following theorem (a proof is given in Appendix A for completeness).

Theorem 1.—Let ν be a quantum (η,t) TPE. Then, iterating the TPE $\ell \ge \{1/[\log(1/\eta)]\}\log(d^t/\epsilon)$ times results in an ϵ-approximate unitary t-design.

III. MAIN RESULTS

Here, we present a summary of our three main results. We first provide implementations of approximate unitary designs on one qudit in Sec. III A. In Sec. III B, we consider N-qubit systems and show that ϵ-approximate unitary t-designs can be implemented by quantum circuits with length $O\{N[tN + \log(1/\epsilon)]\}$. Finally, in Sec. III C, we propose design Hamiltonians and provide a design Hamiltonian with two-body interactions that achieves unitary designs in a short time.

A. One qudit case

We introduce a Fourier-type pair of bases. A pair of orthogonal bases (E, F) is called a Fourier-type pair if each element in $F = \{|\alpha\rangle_F\}_{\alpha\in[0,d-1]}$ is expanded in the basis of $E = \{|k\rangle_E\}_{k\in[0,d-1]}$ as follows:

$$|\alpha\rangle_F = \frac{1}{\sqrt{d}} \sum_{k\in[0,d-1]} e^{i\theta_{k\alpha}} |k\rangle_E, \quad (7)$$

where the phases $\theta_{k\alpha} \in [0, 2\pi)$ satisfy the condition that $\forall k,\ l,\ \alpha \in [0, d-1]$, $\theta_{k+l,\alpha} = \theta_{k\alpha} + \theta_{l\alpha}$. In the index of θ, $+$ should be an additive operation with respect to which $[0, d-1]$ is an additive group. Two important examples of Fourier-type pairs of bases are the following (see Appendix B

for the details): (1) any orthogonal basis $\{|k\rangle\}_{k\in[0,d-1]}$ and its Fourier basis $\{d^{-1/2}\sum_k \omega^{\alpha k}|k\rangle\}_{\alpha\in[0,d-1]}$, where ω is a dth root of unity, and (2) the Pauli-X and Pauli-Z bases on N qubits. These two examples are versions of the position and momentum bases in continuous and discrete spaces, respectively. It is known that if D^W $(W = E, F)$ is applied to the state with a large support in the basis of W, then the resulting state is strongly randomized [58,60]. This fact naturally leads us to expect that alternate applications of D^E and D^F randomize any states and eventually achieve quantum pseudorandomness. This is indeed the case.

Theorem 2.—Let $d = \Omega(t^2 t!^2)$ and (E, F) be a Fourier-type pair of bases. For independent random diagonal unitaries D^E and D'^E in the basis of E and D^F in the basis of F, $D^E D^F D'^E$ is a quantum (η, t) TPE with η given by

$$\eta = \frac{(1+t^2)t!^2 + t^2}{d} + O\left(\frac{t^4 t!^2}{d^2}\right). \tag{8}$$

The proof is given in Sec. IV B. From Theorems 1 and 2, and noticing that applying two random diagonal unitaries in the same basis is equivalent to applying one random diagonal unitary in that basis, we obtain our first main result.

Corollary 3 (Main result 1).—Let (E, F) be a Fourier-type pair of bases and assume that $d = \Omega(t^2 t!^2)$. A random unitary $D[\ell] \coloneqq D^E_\ell D^F_\ell D^E_{\ell-1} D^F_{\ell-1} \ldots D^E_1 D^F_1 D^E_0$, where D^E_i and D^F_i are independent random diagonal unitaries in the basis of E and F, respectively, is an ϵ-approximate unitary t-design if

$$\ell \geq \frac{1}{\log d - 2\log(t!)}[t\log d + \log(1/\epsilon)], \tag{9}$$

up to the leading order of d and t.

This construction of designs works for any space, which is not necessarily a whole tensor-product space, and will be useful when we need designs in certain subspaces. This is the case, for instance, in quantum metrology, where it was recently shown that almost any random symmetric states are useful to demonstrate a quantum advantage [18]. As unitary designs in the symmetric subspace are needed for generating such random states, our construction will help the demonstration of a quantum advantage in metrology. Another interesting instance is an experimental demonstration of self-thermalization in isolated quantum systems, which can be done by applying Haar random unitaries or unitary designs onto the system and the environmental system [19–21]. Since the temperature of the system is determined by the total energy in the system and the environment, unitary designs should act on the subspace with restricted energy. Our construction is suited in this situation because a pair of position and momentum bases of pseudoparticles with fixed energies forms a Fourier-type pair and may be physically feasible to deal with.

Before we proceed to the next section, we make a short remark on the assumption $d = \Omega(t^2 t!^2)$ in Theorem 2 and Corollary 3. This assumption comes from a technical reason and it remains open whether the assumption can be removed (see Sec. IV B for more details).

B. *N*-qubits case

We now focus on N-qubit systems. In particular, we consider applying random diagonal unitaries in the Pauli-X and -Z bases. From Corollary 3, repeating these random diagonal unitaries yields an ϵ-approximate unitary t-design if the number ℓ of repetitions satisfies

$$\ell \geq \frac{1}{N - 2\log_2(t!)}[tN + \log_2(1/\epsilon)], \tag{10}$$

as long as $2^N = \Omega(t^2 t!^2)$. However, this construction is inefficient because an exact implementation of random diagonal unitaires by quantum circuits requires an exponential number of local gates. Thus, we need to find efficient implementations of approximate random diagonal unitaries by quantum circuits. As the Pauli-X and -Z bases are related by the Hadamard transformation, it suffices to consider those only in the Pauli-Z basis.

1. Random diagonal circuits and local permutation checks

We especially study the following family of random diagonal circuits (RDC). Let $\mathcal{I} = \{I_i\}$ be a set of $I_i \subset [1, N]$, and denote $M_i \coloneqq 2^{|I_i|} - 1$. At the ith step of the circuit, we apply a random diagonal gate $\mathrm{diag}_Z\{e^{i\varphi_0}, \ldots, e^{i\varphi_{M_i}}\}$ onto the qubits located in I_i, where the gate is diagonal in the Pauli-Z basis and the phases φ_k $(k \in [0, M_i])$ are chosen independently and uniformly at random from $[0, 2\pi)$ every step. Since the circuit is fully specified by $\mathcal{I}$, we denote it by $\mathrm{RDC}(\mathcal{I})$. We refer to $|\mathcal{I}|$ as the length of the circuit.

The problem of approximating random diagonal unitaries in the Pauli-Z basis by $\mathrm{RDC}(\mathcal{I})$ is related to an elementary combinatorial problem, which may be of interest in its own right. We first introduce the combinatorial problem here, and then show the connection to the original problem.

Let K and K' be $t \times N$ matrices with elements in $\{0, 1\}$. For given $s \in [1, t]$ and $I \subset [1, N]$, we denote a subsequence $(K_{s,m})_{m\in I}$ of the sth row of K by $K_{s,I}$ and a set $\{K_{s,I}\}_{s\in[1,t]}$ of such subsequences over all s by K_I. We use the same notation also for K'. Let Ω be a canonical map that rearranges the subsequences K_I in ascending order, where the subsequences are regarded as binary numbers. For $\mathcal{I} = \{I\}$, we say that K is an $\mathcal{I}$-local permutation of K' if $\forall I \in \mathcal{I}, \Omega(K_I) = \Omega(K'_I)$. In particular, we say K is a row

permutation of K' if $\Omega(K_I) = \Omega(K'_I)$ for $I = [1, N]$, which simply implies that a set of rows of K is a permutation of that of K'. In the following, we denote by $\mathcal{I}_r$ a set of all subsets in $[1, N]$ with r elements. Using this notation, the task of local permutation check problems is to count the number of pairs (K, K') such that K is not a row permutation but an $\mathcal{I}$-local permutation of K'. We denote the number of such pairs by $\Lambda(\mathcal{I})$. In particular, for $\mathcal{I}_r$, we call the problem an r-local permutation check problem and denote the number of pairs by Λ_r. For a couple of examples of local permutation checks, see Fig. 1.

To see the connection between the implementations of quantum TPEs by RDC($\mathcal{I}$) and the $\mathcal{I}$-local permutation check problem, we consider $\mathbb{E}_{D^Z\sim\mathsf{RDC}(\mathcal{I})}[(D^Z)^{\otimes t,t}]$, which is an operator diagonal in the Pauli-Z basis on $(\mathbb{C}^2)^{\otimes tN} \otimes (\mathbb{C}^2)^{\otimes tN}$. We label each vector of the Z basis in $(\mathbb{C}^2)^{\otimes tN}$ by a $t \times N$ matrix K with elements in $\{0, 1\}$ (see Appendix C for further details). Then, we can show that

$$\langle K, K'|\mathbb{E}_{D^Z\sim\mathsf{RDC}(\mathcal{I})}[(D^Z)^{\otimes t,t}]|K, K'\rangle = \begin{cases} 1 & \text{if } K \text{ is an } \mathcal{I}\text{-local permutation of } K' \\ 0 & \text{otherwise.} \end{cases} \quad (11)$$

See Fig. 1(c) as well. Based on this fact, we obtain that, when $2^N = \Omega(t^2 t!^2)$, iterating RDC($\mathcal{I}$) and the Hadamard transformation H_N on N qubits, such as RDC($\mathcal{I}$)H_NRDC($\mathcal{I}$)H_NRDC($\mathcal{I}$) [see Fig. 2(a)], yields a quantum $(\tilde{\eta}, t)$ TPE, where

$$\tilde{\eta} \le \eta + 3t! \frac{\Lambda(\mathcal{I})}{2^{tN}} + \left(\frac{\Lambda(\mathcal{I})}{2^{tN}}\right)^2, \quad (12)$$

with $\eta = [(1 + t^2)t!^2 + t^2]/2^N + O(t^4 t!^2/2^{2N})$ (see Appendix C for the details).

2. Approximating random diagonal unitaries by RDC($\mathcal{I}_2$)

To obtain our second main result, RDC($\mathcal{I}_2$) [see Fig. 2(b)] and the 2-local permutation check problem are of particular importance. Because of the result in Ref. [61], we know that $\Lambda_2 = 0$ for $t \le 3$. When $t \ge 4$, the problem can be rephrased as an extremal problem under dimension constraints, which is a constrained problem in extremal algebraic theory [62,63]. By solving a special case of the problem (see Sec. IV C), we obtain $\Lambda_2 \le 2^{2t^2+(t-1)N}$. Thus, for $t = o(N^{1/2})$, iterating RDC($\mathcal{I}_2$) and the Hadamard transformation is a quantum $(\tilde{\eta}, t)$ TPE, where

$$\tilde{\eta} \le 2^{2t^2+2-N} t! + O(t^2 t!^2 2^{-N}), \quad (13)$$

from which we obtain an efficient implementation of a unitary t-design due to Theorem 1.

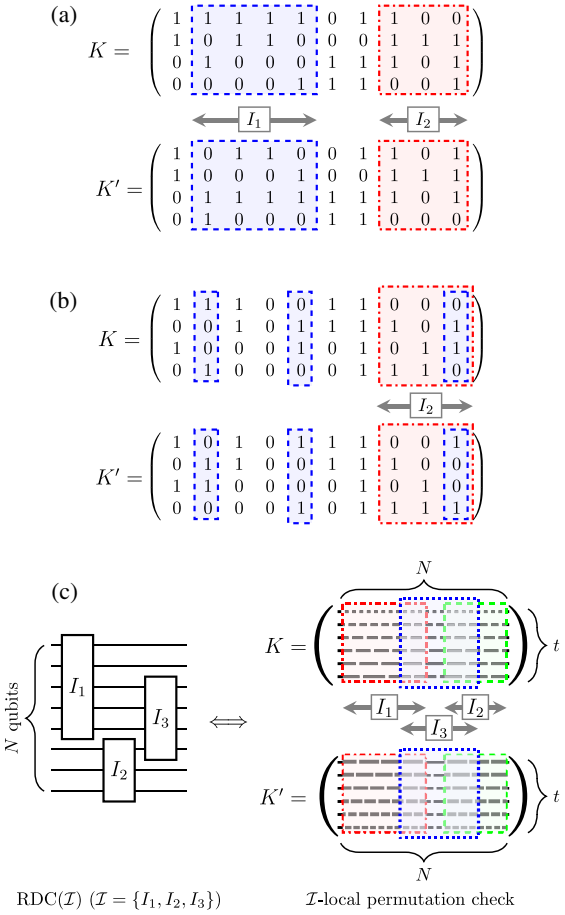

FIG. 1. (a),(b) Examples of local permutation check problems for $t = 4$ and $N = 10$. In (a), $K_{I_1} = \{1111, 0110, 1000, 0001\}$ is a permutation of $K'_{I_1} = \{0110, 0001, 1111, 1000\}$ (blue dashed boxes). However, K_{I_2} is not a permutation of K'_{I_2} (red dash-dotted boxes). Hence, K is an $\{I_1\}$-local but not an $\{I_2\}$-local permutation of K', also implying that K is not a row permutation of K'. In (b), K is identical to K' except the columns in the blue dashed boxes and is a 2-local permutation of K'. However, K fails to be a 3-local permutation of K' due to the last column (see, e.g., K_{I_2} and K'_{I_2}). Panel (c) illustrates a relation between RDC($\mathcal{I}$) and an $\mathcal{I}$-local permutation check problem. As diagonal gates act on I_1, I_2, and I_3, we first check if K is a $\{I_1, I_2, I_3\}$-local permutation of K'. That is, we check the permutation relations between sets of rows in the red dash-dotted, green dotted, and blue dashed boxes. If K is $\{I_1, I_2, I_3\}$-local but not a row permutation of K', then $\langle K, K'|\mathbb{E}_{D^Z\sim\mathsf{RDC}(\mathcal{I})}[(D^Z)^{\otimes t,t}]|K, K'\rangle = 1$.

We can further reduce the number of randomness in the implementation by replacing all gates in RDC($\mathcal{I}_2$) with those in the form of

$$(\mathrm{diag}\{1, e^{i\varphi_1}\} \otimes \mathrm{diag}\{1, e^{i\varphi_2}\})\mathrm{diag}\{1, 1, 1, e^{i\vartheta}\}. \quad (14)$$

When φ_1 and φ_2 are chosen independently from $\{2\pi m/a : m \in [0, a-1]\}$ uniformly at random, and ϑ is chosen from $\{2\pi m/b : m \in [0, b-1]\}$, we denote the circuit $\mathrm{RDC}_{\mathrm{disc}}(\mathcal{I}_2 : a, b)$. Using the same technique as in

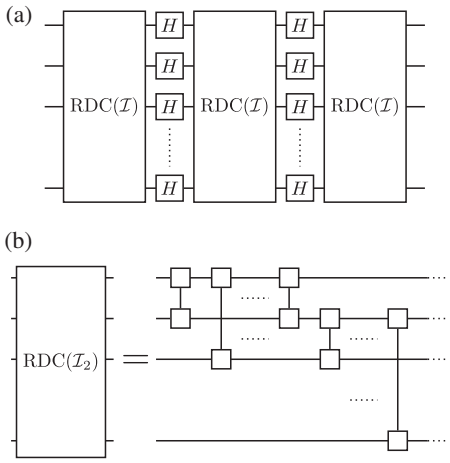

FIG. 2. Panel (a) depicts iterations of RDC($\mathcal{I}$) and the Hadamard transformation. Panel (b) shows RDC($\mathcal{I}_2$), where random diagonal two-qubit gates are applied onto all pairs. The circuit is called $\mathrm{RDC}^{(t)}_{\mathrm{disc}}(\mathcal{I}_2)$ when each two-qubit gate is replaced with $(\mathrm{diag}_Z\{1, e^{i\varphi_1}\} \otimes \mathrm{diag}_Z\{1, e^{i\varphi_2}\})\mathrm{diag}_Z\{1, 1, 1, e^{i\vartheta}\}$, where the phases ϕ_1, ϕ_2 and ϑ are chosen from discrete sets given in the main text.

Ref. [61], we obtain that if $a \geq t+1$ and $b \geq \lfloor t/2 \rfloor + 1$, $\mathrm{RDC}_{\mathrm{disc}}(\mathcal{I}_2 : a, b)$ simulates up to the tth-order moments of RDC($\mathcal{I}_2$). In particular, we denote $\mathrm{RDC}_{\mathrm{disc}}(\mathcal{I}_2 : t+1, \lfloor t/2 \rfloor + 1)$ simply by $\mathrm{RDC}^{(t)}_{\mathrm{disc}}(\mathcal{I}_2)$, where one two-qubit gate requires $2\log_2(t+1)+\log_2(\lfloor t/2 \rfloor + 1) < 3\log_2(t+1)$ random bits. Together with all of these, we obtain our second main result.

Theorem 4 (Main result 2).—For $t = o(N^{1/2})$, iterating $\mathrm{RDC}^{(t)}_{\mathrm{disc}}(\mathcal{I}_2)$ and the Hadamard transformation on N qubits, such as $[\mathrm{RDC}^{(t)}_{\mathrm{disc}}(\mathcal{I}_2)H_N]^{2\ell}\mathrm{RDC}^{(t)}_{\mathrm{disc}}(\mathcal{I}_2)$, yields an ϵ-approximate unitary t-design if

$$\ell \geq t + \frac{1}{N}\log_2(1/\epsilon), \tag{15}$$

up to the leading order of N and t. The total number of two-qubit gates and random bits are given by

$$\text{no. of two-qubit gates} = \Theta\{N[tN + \log_2(1/\epsilon)]\}, \tag{16}$$

$$\text{no. of random bits} = \Theta\{(\log_2 t)N[tN + \log_2(1/\epsilon)]\}, \tag{17}$$

respectively.

We assume in Theorem 4 that $t = o(N^{1/2})$. However, we believe that Theorem 4 holds even for $t = o(N/\log N)$, which comes from the conjecture we explain in more detail in Sec. IV C.

In terms of t, Theorem 4 drastically improves the previous result using $O\{t^9 N[tN + \log(1/\epsilon)]\}$ two-qubit gates [35,43] (see also Table I for the comparison) and is essentially optimal when the design is defined on a finite set of unitaries. This is because the support of a unitary t-design should contain at least $O(2^{2tN})$ unitaries [64]. Thus, when each gate in a random quantum circuit is chosen from a finite set, the scaling of the length necessary for the circuit achieving a t-design cannot be substantially better than linear in t.

In practical uses of unitary designs, such as decoupling [5–8] and randomized benchmarking [9–12], unitary 2-designs are known to be sufficient, for which a more efficient construction by Clifford circuits with length $O(N\log^2 N)$ is known [44]. However, unitary 4-designs are needed in a few applications [13–15], which cannot be achieved by any Clifford circuit [46]. Moreover, higher designs are generally more useful than lower designs because they have stronger large deviation bounds [56], which are finite approximations of the concentration of measure for Haar random unitaries stating that values of any slowly varying function on a unitary group are likely to be almost constant if the dimension is large [65]. This implies that using higher designs in any applications of unitary designs results in better performance. Since our implementation provides a quantum circuit for t-designs shorter than the existing ones [34,35,43], it contributes to improving the performance of quantum protocols using quantum pseudorandomness [1–16,18].

This construction of approximate designs also has advantages from an experimental point of view. As highlighted in Refs. [45,55], the quantum circuits repeating RDC($\mathcal{I}_2$) or $\mathrm{RDC}^{(t)}_{\mathrm{disc}}(\mathcal{I}_2)$ and the Hadamard transformation are divided into a constant number of commuting parts.

TABLE I. A comparison between quantum circuit constructions of unitary t-designs on N qubits, which works for $t \geq 3$. The total number of quantum gates to achieve classical tensor expanders is known to be poly(N), but is not explicitly presented in Ref. [33]. The noncommuting depth was introduced in Ref. [55] and is defined by the circuit depth when each commuting part of the circuit is counted as one step. The noncommuting depth may be of experimental importance.

	Total number of gates	t	Noncommuting depth [55]
Classical tensor expanders [33]	poly(N)	$O(N/\log N)$	poly(N)
Local random circuits [35,43]	$O\{t^9 N[tN + \log(1/\epsilon)]\}$	poly(N)	$O\{t^9[tN + \log(1/\epsilon)]\}$
Random diagonal circuits	$O\{N[tN + \log_2(1/\epsilon)]\}$	$o(N^{1/2})$	$O[t + (1/N)\log_2(1/\epsilon)]$

Indeed, only noncommuting parts are the Hadamard parts. Because the gates in each commuting part do not have any temporal order, they can be applied simultaneously in experimental realizations, possibly making the actual implementation time shorter. Hence, the commuting structure of our construction may help reduce the practical time and increase the robustness of the implementations. This property can be rephrased in terms of the noncommuting depth proposed in Ref. [55] (see Table I).

C. Hamiltonian dynamics and unitary designs

In the past decade, quantum randomness was revealed to be the key to understanding fascinating phenomena in complex quantum many-body systems [19–28], in most of which the dynamics is assumed to be so random that it can be described by Haar random unitaries or unitary designs. This assumption may be reasonable as a first approximation. However, due to the lack of full understanding of natural microscopic dynamics generating unitary designs, it is not clear to what extent the assumption can be justified.

Most recently, the idea of scrambling was introduced in black hole information science [23,24]. The main concern there is the fast scrambling conjecture, stating that the shortest time necessary for natural dynamics to scramble many-body systems scales logarithmically with the system size [24–28]. While it is known that 0-dimensional systems, where all particles interact with each other, can be scrambled in a constant time [66], the conjecture is strongly believed to hold in higher dimensions. The fast scrambling conjecture originally arose from a thought experiment concerning the black hole evaporation and the no-cloning theorem [24], but has also been studied intensely in connection with quantum chaos [29–31]. So far, several inequivalent definitions of scrambling have been proposed [24,26,28]. Although they are useful for clarifying the relationship between scrambling and other notions of randomization, such as unitary designs and the OTO correlators diagnosing quantum chaos [29–31], there does not seem to be consensus on a rigorous mathematical definition of scrambling.

Here, we introduce design Hamiltonians as a unifying framework for studying natural microscopic dynamics of quantum randomness. In terms of the design Hamiltonians, we generalize the fast scrambling conjecture and propose a natural design Hamiltonian conjecture. We then construct a design Hamiltonian, where the interactions need to be changed only a few times before the corresponding dynamics form unitary designs. This is in sharp contrast to the Hamiltonian dynamics based on local random quantum circuits [35,43], which we elaborate on later.

1. Design Hamiltonians

We especially consider k-local Hamiltonians [57] on N qubits, $H = \sum_i H_i$. Here, each term H_i may be dependent on time, $\|H_i\|_\infty \leq 1$, and acts nontrivially only on the qubits in $\Lambda_i \subset [1, N]$, which satisfies $|\Lambda_j| \leq k$ and $\Lambda_i \neq \Lambda_j$ if $i \neq j$. We denote by $\mathfrak{H}_k$ a set of all k-local Hamiltonians. The interactions in k-local Hamiltonians are not necessarily geometrically local on lattice systems. They are, rather, interpreted as interactions on a given graph, where each vertex represents a particle. To normalize the time scale of the dynamics, we also assume that the strength of each local interaction is bounded. In the following, to avoid confusion, we always use small t and capital T for t-designs and time, respectively. We denote $U_H(T) \coloneqq \mathcal{T}\exp[-i\int_0^T dsH(s)]$, where $\mathcal{T}\exp$ is the time-ordered exponential, the time evolution operator at time T generated by a possibly time-dependent Hamiltonian H. An ϵ-approximate t-design Hamiltonian with k-local interaction is a random k-local Hamiltonian H, where there exists $T_0 > 0$ such that, for any $T \geq T_0$, a random unitary $U_H(T)$ generated by H is an ϵ-approximate unitary t-design. We call the shortest such time T_0 a design time of H (see Fig. 3 for intuitive illustrations).

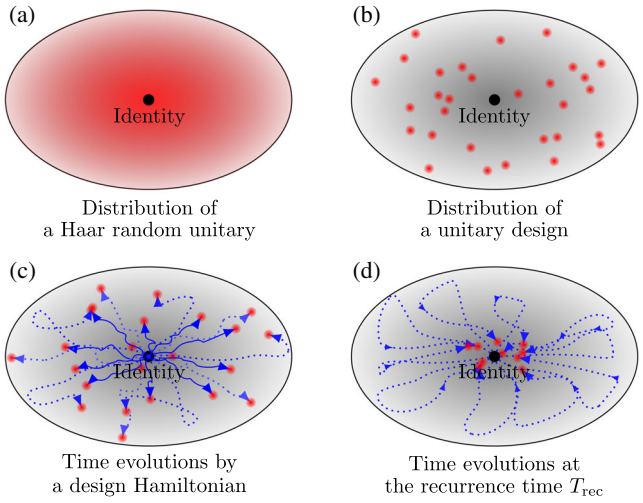

FIG. 3. Schematic figures illustrating the distributions of random unitaries in a whole unitary group. For the visualization, the unitary group is represented by an ellipse and each red dot corresponds to a unitary operator. Panel (a) illustrates a Haar random unitary, which is uniformly and continuously distributed over the whole unitary group. For unitary designs, the distribution is not necessarily continuous and is often defined on a finite support, which is depicted in (b). Panel (c) provides an intuitive picture of time-evolution operators generated by a design Hamiltonian, starting from the identity. As time passes, a design Hamiltonian generates random unitary distributed over the whole unitary. The time evolution is illustrated by a trajectory in the panel. When the design Hamiltonian is defined on a finite ensemble of Hamiltonians, there exists a time $T_{\rm rec}$, where all time evolution operators are in the neighborhood of the identity, due to the Poincaré recurrence theorem as depicted in (d).

This definition of design Hamiltonians is a little strong and can be weakened if necessary. Indeed, there is no design Hamiltonian in this sense on a finite ensemble of time-independent Hamiltonians. Because of the Poincaré recurrence theorem [67], the time-evolution operator generated by a time-independent Hamiltonian is in the

neighborhood of the identity operator at the recurrence time. Although the time-evolution operators generated by other Hamiltonians are possibly not close to the identity at the recurrence time of one Hamiltonian, we can always find the time T_{rec} where all operators are close to the identity. Hence, at that time T_{rec}, an ensemble of time-evolution operators does not form unitary designs (see also Fig. 3). However, this problem can be avoided if we consider time-dependent Hamiltonians or a continuous ensemble of time-independent Hamiltonians. We can also relax the condition of $\forall T \geq T_0$ to most of the time after T_0.

2. Natural design Hamiltonian conjecture

As our main purpose is to find physically natural Hamiltonians generating unitary designs, we are most interested in the design Hamiltonians that are not finely structured, are time independent, and are with geometrically local interactions. In addition, we may further require that, due to the fast scrambling conjecture, the design time scales logarithmically with the system size, which may depend on t. Thus, we arrive at the natural design Hamiltonian conjecture that there exist ϵ-approximate t-design Hamiltonians on N qubits that satisfy the following three conditions: (1) the interactions are geometrically local, (2) the interactions are all time independent, and (3) the design time is given by $O(t \log N)$, which may also depend on ϵ.

In general, the Hamiltonians with random interactions are expected to exhibit many-body localization [68–70], preventing the corresponding dynamics from achieving unitary designs quickly. However, this is not always the case. For instance, the dynamics of a Majorana fermion model with random four-body interactions, also known as the Sachdev-Ye-Kitaev (SYK) model [71,72], is known to be strongly chaotic [73,74] and is likely to achieve unitary designs at least on the low-energy subspace. Although the SYK model consists of all-to-all interactions and does not meet the first condition of the conjecture, further investigation of this model may help in the search of natural design Hamiltonians satisfying all three conditions.

The conjecture is based on an established language of unitary designs and so will be helpful to explore randomizing operations in physically natural systems in a mathematically rigorous manner. We note that the conjecture is not only of theoretical interest but also of practical importance because, by applying such a random Hamiltonian onto a system, a unitary design will be spontaneously obtained. Most importantly, there is no need to change the interactions and no fine control of time is required. This will drastically simplify the implementations of unitary designs in experiments, also resulting in the simplification of many quantum protocols [1–16,18].

The construction of designs by local random quantum circuits [35,43] can be naturally translated into design Hamiltonians: a random Hamiltonian with neighboring two-body interactions is a t-design Hamiltonian if the interactions vary randomly and independently at every time step. Such varying interactions can be considered to be fluctuations induced by white noise on two-body interactions [75]. This design Hamiltonian H_{rand} satisfies the first condition of the conjecture, as it uses only neighboring interactions, but not the second and the third ones. Indeed, to achieve a unitary t-design by the dynamics of H_{rand}, the interactions should be changed $O(t^{10}N)$ times uniformly at random. This is far from time independent and takes much longer than $O(t \log N)$. Here, we are more concerned with the second condition of the conjecture and provide a design Hamiltonian H_{XZ} based on Theorem 4.

3. Design Hamiltonian H_{XZ}

We first introduce a parameter set $\mathcal{P}_t(c)$ by

$$\mathcal{P}_t(c) = \left\{ \frac{m}{2(\lfloor t/2 \rfloor + 1)} : m \in [-c, c] \right\}. \tag{18}$$

Our design Hamiltonian consists of two types of disordered commuting Hamiltonians, which may appear in many-body localized systems [68–70]:

$$\mathfrak{H}_Z^{(t)} := \left\{ -\sum_{j<k} J_{ik} Z_j \otimes Z_k - \sum_j B_j Z_j \right\}_{J_{jk}, B_j}, \tag{19}$$

$$\mathfrak{H}_X^{(t)} := \left\{ -\sum_{j<k} J_{ik} X_j \otimes X_k - \sum_j B_j X_j \right\}_{J_{jk}, B_j}, \tag{20}$$

where the coefficients J_{jk} and B_j are chosen from $\mathcal{P}_t(J)$ and $\mathcal{P}_t(B)$, where $J = [(\lfloor t/2 \rfloor)/2]$ and $B = \lfloor t/2 \rfloor + \frac{1}{2}$, respectively. Our third main result is that alternate applications of H_Z randomly chosen from $\mathfrak{H}_Z^{(t)}$ and H_X randomly chosen from $\mathfrak{H}_X^{(t)}$ are a design Hamiltonian. To be precise, we introduce a notation $\in_R$, which implies that the left-hand side is drawn uniformly at random from the set in the right-hand side. Then, our third main result is given as follows.

Corollary 5 (Main result 3).—Let $t = o(N^{1/2})$ and $\mathfrak{H}_{XZ}^{(t)}$ be a set of 2-local time-dependent Hamiltonians in the form of

$$H_{XZ}(T) = \begin{cases} H_Z^{(m)} & \text{if } \ 2m\pi \leq T < (2m+1)\pi \\ H_X^{(m)} & \text{if } \ (2m+1)\pi \leq T < 2(m+1)\pi, \end{cases} \tag{21}$$

where T denotes time, and $H_W^{(m)} \in \mathfrak{H}_W^{(t)}$ for any $m = 0, 1, \ldots$ $(W = X, Z)$. Then, the random Hamiltonian $H_{XZ} \in_R \mathfrak{H}_{XZ}^{(t)}$ is an ϵ-approximate t-design Hamiltonian. The design time of H_{XZ} is at most $[2t + 1 + (2/N)\log_2(1/\epsilon)]\pi$.

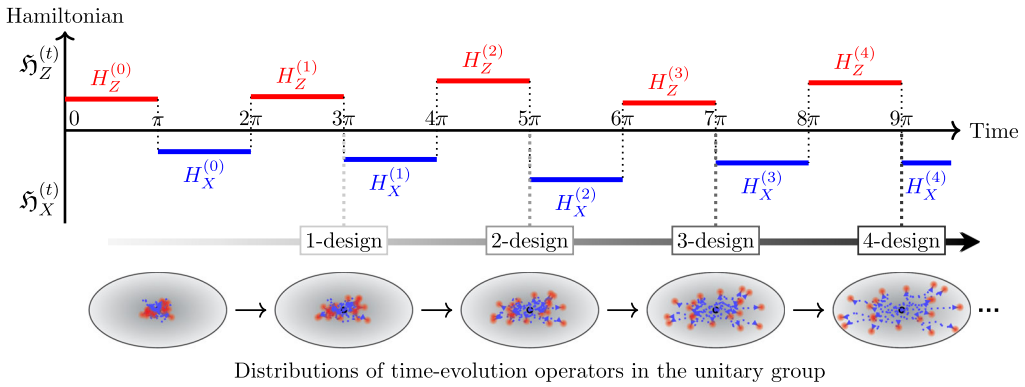

FIG. 4. A schematic figure about the design Hamiltonian $H_{XZ} \in_R \mathfrak{H}_{XZ}^{(t)}$. At each time interval m, $H_Z^{(m)}$ or $H_X^{(m)}$ is chosen uniformly at random from $\mathfrak{H}_Z^{(t)}$ or $\mathfrak{H}_X^{(t)}$, respectively. As depicted at the bottom of the figure, a random unitary generated by H_{XZ} rapidly spreads over the whole unitary group and forms unitary designs in a short time independent of the system size.

Since H_{XZ} is composed of H_Z and H_X, both of which exhibit many-body localization, one may think that the time-evolution operators generated by $H_{XZ} \in_R \mathfrak{H}_{XZ}^{(t)}$ shall not spread over the whole unitary group. However, due to the periodic change of the interaction basis, the localization indeed helps the time-evolution operators to be uniform. This can be observed from the fact that a random unitary diagonal in a fixed basis has a strong randomization power when the initial state has a large support in that basis [58,60]. Since a localized state in one basis has a large support in the complementary basis, the time evolution by H_Z (H_X) randomizes the localized eigenstates of H_X (H_Z) strongly. For this reason, it is natural to expect that the time-evolution operators generated by H_{XZ} eventually form a unitary design, which can be rigorously proven in Corollary 5. Technically, Corollary 5 is obtained by interpreting Theorem 4 in terms of the Hamiltonian dynamics and using the fact that, if U is an ϵ-approximate unitary t-design, then VU is also an ϵ-approximate unitary t-design for a random unitary V independent of U. For the details, see Sec. IV D.

Note that our specific choice of the parameters in the Hamiltonians H_Z and H_X, namely, $J_{jk} \in_R \mathcal{P}_t(J)$ and $B_j \in_R \mathcal{P}_t(B)$, is to minimize the randomness needed to construct a design Hamiltonian. It is possible to choose the parameters from different sets as long as they are sufficiently random, where the design time will be accordingly changed. From a physical point of view, it may be interesting to consider physically feasible noises as parameter sets, which is in the same spirit as Ref. [75].

We observe from Corollary 5 that the time evolution generated by $H_{XZ} \in_R \mathfrak{H}_{XZ}^{(t)}$ quickly becomes hard to distinguish from a completely random one (see also Fig. 4). Most notably, the design time is $O(t)$ and independent of the system size. As a simple consequence, any correlation functions at time T in the system described by such a Hamiltonian quickly converge to the Haar averaged values. One of the important instances is the $2t$-point OTO correlator, which is expected to diagnose quantum chaos and has been studied in strongly correlated systems [29–31]. As the $2t$-point OTO correlators are polynomials of a unitary with degree t, their values in the system of a random Hamiltonian H_{XZ} are ϵ close to the Haar random averages when $T \gtrsim [2t + 1 + (2/N)\log_2(1/\epsilon)]\pi$. Furthermore, due to the large deviation bounds for unitary designs [56], this implies that almost any Hamiltonian in $\mathfrak{H}_{XZ}^{(t)}$ saturates the $2t$-point OTO correlators to the Haar random averages in a short time irrespective of the system size. As the OTO correlators are saturated in quantum chaotic systems [28], our result indicates a close connection between the Hamiltonians in $\mathfrak{H}_{XZ}^{(t)}$ and quantum chaos, which suggests that the framework of design Hamiltonians may be useful to investigate the dynamics in quantum chaotic systems. This is also supported by a recently clarified relation between unitary designs and quantum chaos [76].

TABLE II. A comparison of design Hamiltonians, H_{rand} [35,43] and H_{XZ}, in terms of the three conditions of the natural design Hamiltonian conjecture. The design time of H_{XZ} is much shorter than that of H_{rand}, both in terms of t and N. Although the improvement in terms of t is generic to H_{XZ}, that in terms of N is probably due to its all-to-all interactions (see the main text).

Design Hamiltonian	Interactions	Time dependence	Design time
H_{rand}	Nearest-neighbor interactions	Highly dependent	$O(t^{10}N)$
H_{XZ}	All-to-all two-body interactions	Nearly time independent	$O(t)$

In Table II, we compare two design Hamiltonians $H_{\rm rand}$ and H_{XZ}. We emphasize that the design time $O(t)$ of H_{XZ} is significantly faster than the design time $O(t^{10}N)$ of $H_{\rm rand}$ in terms of both t and N. We should note, however, that although the improvement in terms of t is intrinsic to H_{XZ}, the improvement in terms of N may be, rather, due to the all-to-all interactions of H_{XZ}. Such interactions may naturally appear in cavity QED [77–79] due to the cavity modes mediating long-range interactions, and unitary designs may possibly be realized in a constant time. Nevertheless, for a fair comparison with $H_{\rm rand}$, the realization of all-to-all interactions by neighboring ones should be taken into account. This can be achieved if every particle travels all corners of the system and interacts with all the other particles, taking $O(N)$ time. Hence, when the interactions are neighboring, the actual time for H_{XZ} to generate unitary designs is considered to be $O(tN)$, also implying that it does not violate the fast scrambling conjecture.

Unfortunately, both design Hamiltonians $H_{\rm rand}$ and H_{XZ} do not satisfy all three conditions of the natural design Hamiltonian conjecture. However, we believe that the existence of two design Hamiltonians $H_{\rm rand}$ and H_{XZ} and previous analyses on the original fast scrambling conjecture [24–28] provide substantial evidence for the natural design Hamiltonian conjecture.

IV. PROOFS

In this section, we provide proofs of our main results given in Sec. III. We first introduce additional notation and useful lemmas in Sec. IV A. The proof of our first main result, Theorem 2, is given in Sec. IV B. We prove the key lemma to obtain our second main result in Sec. IV C, and conclude this section by showing Corollary 5 about design Hamiltonians in Sec. IV D.

A. Additional notation

Let $E=\{|k\rangle_E\}_{k\in[0,d-1]}$ and $F=\{|\alpha\rangle_F\}_{\alpha\in[0,d-1]}$ be orthogonal bases in a d-dimensional Hilbert space $\mathcal{H}$. As we deal with t copies of the Hilbert space $\mathcal{H}^{\otimes t}$, we denote $[0,d-1]^t$ by $\mathcal{N}$ and introduce bases $\{|\mathbf{k}\rangle_W\}_{\mathbf{k}\in\mathcal{N}}$ $(W=E,F)$ in $\mathcal{H}^{\otimes t}$, where $|\mathbf{k}\rangle_W=\bigotimes_{s=1}^{t}|k_s\rangle_W$, $\mathbf{k}=(k_1,\ldots,k_t)^T\in\mathcal{N}$, and T represents the transpose. In the following, we always label the basis E and F by latin and greek alphabets, respectively, and do not write the subscript E and F explicitly.

Let S_t be a permutation group of degree t. For $\pi\in S_t$, we denote $(k_{\pi^{-1}(1)},\ldots,k_{\pi^{-1}(t)})^T$ by $\mathbf{k}_\pi$, and define a state $|\Psi_\pi\rangle\in\mathcal{H}^{\otimes 2t}$ by

$$|\Psi_\pi\rangle := I\otimes V(\pi)|\Phi\rangle \tag{22}$$

$$=\frac{1}{d^{t/2}}\sum_{\mathbf{k}\in\mathcal{N}}|\mathbf{k},\mathbf{k}_\pi^*\rangle \tag{23}$$

$$=\frac{1}{d^{t/2}}\sum_{\boldsymbol{\alpha}\in\mathcal{N}}|\boldsymbol{\alpha},\boldsymbol{\alpha}_\pi^*\rangle, \tag{24}$$

where $V(\pi)$ is a unitary representation of π, $|\Phi\rangle$ is the maximally entangled state between the first $\mathcal{H}^{\otimes t}$ and the second $\mathcal{H}^{\otimes t}$, $|\mathbf{k},\mathbf{k}_\pi^*\rangle=|\mathbf{k}\rangle\otimes(|\mathbf{k}_\pi\rangle)^*$, and $|\boldsymbol{\alpha},\boldsymbol{\alpha}_\pi^*\rangle=|\boldsymbol{\alpha}\rangle\otimes(|\boldsymbol{\alpha}_\pi\rangle)^*$. Note that $|\Psi_\pi\rangle$ and $|\Psi_\sigma\rangle$ are not necessarily orthogonal depending on the permutation element. We denote $|\Psi_\pi\rangle\langle\Psi_\pi|$ simply by Ψ_π.

We also introduce three subspaces in $\mathcal{H}^{\otimes 2t}$:

$$\mathcal{H}_E=\mathrm{span}\{|\mathbf{k},\mathbf{k}_\pi^*\rangle:\mathbf{k}\in\mathcal{N},\pi\in S_t\}, \tag{25}$$

$$\mathcal{H}_F=\mathrm{span}\{|\boldsymbol{\alpha},\boldsymbol{\alpha}_\pi^*\rangle:\boldsymbol{\alpha}\in\mathcal{N},\pi\in S_t\}, \tag{26}$$

$$\mathcal{H}_0=\mathrm{span}\{|\Psi_\pi\rangle:\pi\in S_t\}. \tag{27}$$

Obviously, $\mathcal{H}_E\supsetneq\mathcal{H}_0$ and $\mathcal{H}_F\supsetneq\mathcal{H}_0$. The projectors onto the subspaces $\mathcal{H}_E$, $\mathcal{H}_F$, and $\mathcal{H}_0$ are denoted by P_E, P_F, and P_0, respectively. We further introduce an equivalent relation $\sim_{\mathbf{k}}$ $(\mathbf{k}\in\mathcal{N})$ in S_t such that $\pi\sim_{\mathbf{k}}\sigma$ if and only if $\mathbf{k}_\pi=\mathbf{k}_\sigma$. A set of representative elements in equivalence classes by $\sim_{\mathbf{k}}$ is denote by $S_t^{\mathbf{k}}$. Using this notation, the projectors P_E and P_F are explicitly given by

$$P_E=\sum_{\mathbf{k}\in\mathcal{N}}\sum_{\pi\in S_t^{\mathbf{k}}}|\mathbf{k},\mathbf{k}_\pi^*\rangle\langle\mathbf{k},\mathbf{k}_\pi^*|, \tag{28}$$

$$P_F=\sum_{\boldsymbol{\alpha}\in\mathcal{N}}\sum_{\pi\in S_t^{\boldsymbol{\alpha}}}|\boldsymbol{\alpha},\boldsymbol{\alpha}_\pi^*\rangle\langle\boldsymbol{\alpha},\boldsymbol{\alpha}_\pi^*|. \tag{29}$$

These projectors have the following properties [35,43,61]:

$$\mathbb{E}_{U\sim\mathsf{H}}[U^{\otimes t,t}]=P_0, \tag{30}$$

$$\mathbb{E}_{D^E\sim\mathsf{D}_E}[(D^E)^{\otimes t,t}]=P_E, \tag{31}$$

$$\mathbb{E}_{D^F\sim\mathsf{D}_F}[(D^F)^{\otimes t,t}]=P_F, \tag{32}$$

and

$$\|P_0-\sum_{\pi\in S_t}\Psi_\pi\|_\infty\le\frac{t^2}{d}. \tag{33}$$

B. Proof of the first main result

We now prove Theorem 2. Because of the independence of random diagonal unitaries D^E, D'^E, and D^F and Eqs. (30)–(32), we have

$$\|\mathbb{E}[(D^E D^F D'^E)^{\otimes t,t}] - \mathbb{E}[U^{\otimes t,t}]\|_\infty = \|P_E P_F P_E - P_0\|_\infty, \tag{34}$$

where the averages in the left-hand side are taken over all random unitaries independently. Using the triangular inequality, the fact that $|\Psi_\pi\rangle \in \mathcal{H}_0 \subset \mathcal{H}_E$, and Eq. (33), this is bounded from above as follows:

$$\|P_E P_F P_E - P_0\|_\infty \tag{35}$$

$$\leq \|P_E P_F P_E - \sum_{\pi\in S_t} \Psi_\pi\|_\infty + \|P_0 - \sum_{\pi\in S_t} \Psi_\pi\|_\infty \tag{36}$$

$$\leq \|P_E \left(P_F - \sum_{\pi\in S_t} \Psi_\pi\right) P_E\|_\infty + \frac{t^2}{d}. \tag{37}$$

Since the operator norm for Hermitian operators is bounded from above by the row norm, defined by $\max_j \sum_i |A_{ij}|$ for a Hermitian operator A, we have

$$\|\mathbb{E}[(D^E D^F D'^E)^{\otimes t,t}] - \mathbb{E}[U^{\otimes t,t}]\|_\infty \leq C, \tag{38}$$

where

$$C = \max_{\substack{\mathbf{l}\in\mathcal{N}\\ \sigma\in S_t^{\mathbf{l}}}} \sum_{\substack{\mathbf{k}\in\mathcal{N}\\ \chi\in S_t^{\mathbf{k}}}} |\langle \mathbf{l}, \mathbf{l}_\sigma^*| P_F - \sum_{\pi\in S_t} \Psi_\pi |\mathbf{k}, \mathbf{k}_\chi^*\rangle| + \frac{t^2}{d}. \tag{39}$$

Note that it suffices to consider only vectors in $\mathcal{H}_E^{\otimes t,t}$ when we compute the first term of Eq. (37), which is because the operator is sandwiched by the projector P_E. In the following, we evaluate C.

Substituting $|\Psi_\pi\rangle = (1/\sqrt{d^t})\sum_{\mathbf{m}\in\mathcal{N}} |\mathbf{m}, \mathbf{m}_\pi^*\rangle$, the second term is given by

$$\langle \mathbf{l}, \mathbf{l}_\sigma^*| \sum_{\pi\in S_t} \Psi_\pi |\mathbf{k}, \mathbf{k}_\chi^*\rangle = \frac{1}{d^t} \sum_{\pi\in S_t} \delta_{\mathbf{l}_\pi,\mathbf{l}_\sigma} \delta_{\mathbf{k}_\pi,\mathbf{k}_\chi}. \tag{40}$$

On the other hand, using an explicit form of P_F given in Eq. (29), the first term can be expanded to be

$$\langle \mathbf{l}, \mathbf{l}_\sigma^*| P_F |\mathbf{k}, \mathbf{k}_\chi^*\rangle = \sum_{\boldsymbol{\alpha}\in\mathcal{N}} \sum_{\pi\in S_t^{\boldsymbol{\alpha}}} \langle \mathbf{l}|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|\mathbf{k}\rangle \langle \mathbf{k}_{\pi^{-1}\circ\chi}|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|\mathbf{l}_{\pi^{-1}\circ\sigma}\rangle. \tag{41}$$

Since a pair of the bases (E, F) is a Fourier-type pair, it satisfies for any l, k, $\alpha \in [0, d-1]$ that $\langle l|\alpha\rangle\langle k|\alpha\rangle = \langle l+k|\alpha\rangle/d^{1/2}$, where $l+k \in [0, d-1]$ as $[0, d-1]$ is an additive group with respect to $+$. Denoting $(l_1+k_1, \ldots, l_t+k_t)^T$ by $\mathbf{l}+\mathbf{k}$, we have

$$\langle \mathbf{l}, \mathbf{l}_\sigma^*| P_F |\mathbf{k}, \mathbf{k}_\chi^*\rangle \tag{42}$$

$$= \frac{1}{d^t} \sum_{\boldsymbol{\alpha}\in\mathcal{N}} \sum_{\pi\in S_t^{\boldsymbol{\alpha}}} \langle \mathbf{l} + \mathbf{k}_{\pi^{-1}\circ\chi}|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|\mathbf{k} + \mathbf{l}_{\pi^{-1}\circ\sigma}\rangle \tag{43}$$

$$= \frac{1}{d^t} \sum_{\boldsymbol{\alpha}\in\mathcal{N}} \left(\sum_{\pi\in S_t} - \sum_{\pi\in S_t\setminus S_t^{\boldsymbol{\alpha}}}\right) \langle \mathbf{l} + \mathbf{k}_{\pi^{-1}\circ\chi}|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|\mathbf{k} + \mathbf{l}_{\pi^{-1}\circ\sigma}\rangle \tag{44}$$

$$= \frac{1}{d^t} \left(\sum_{\pi\in S_t} \delta_{\mathbf{l}+\mathbf{k}_{\pi^{-1}\circ\chi},\mathbf{k}+\mathbf{l}_{\pi^{-1}\circ\sigma}} - M_{\mathbf{l},\mathbf{k}}\right), \tag{45}$$

where

$$M_{\mathbf{l},\mathbf{k}} = \sum_{\boldsymbol{\alpha}\in\mathcal{N}} \sum_{\pi\in S_t\setminus S_t^{\boldsymbol{\alpha}}} \langle \mathbf{l} + \mathbf{k}_{\pi^{-1}\circ\chi}|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|\mathbf{k} + \mathbf{l}_{\pi^{-1}\circ\sigma}\rangle, \tag{46}$$

and we use $\sum_{\boldsymbol{\alpha}\in\mathcal{N}} |\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}| = I_{\mathcal{H}^{\otimes t}}$. Hence, we obtain

$$\left|\langle \mathbf{l}, \mathbf{l}_\sigma^*| P_F - \sum_{\pi\in S_t} \Psi_\pi |\mathbf{k}, \mathbf{k}_\chi^*\rangle\right| \tag{47}$$

$$= \frac{1}{d^t} \left|\sum_{\pi\in S_t} (\delta_{\mathbf{l}+\mathbf{k}_{\pi^{-1}\circ\chi},\mathbf{k}+\mathbf{l}_{\pi^{-1}\circ\sigma}} - \delta_{\mathbf{l}_\pi,\mathbf{l}_\sigma}\delta_{\mathbf{k}_\pi,\mathbf{k}_\chi}) - M_{\mathbf{l},\mathbf{k}}\right| \tag{48}$$

$$\leq \frac{1}{d^t} \left|\sum_{\pi\in S_t} (\delta_{\mathbf{l}+\mathbf{k}_{\pi^{-1}\circ\chi},\mathbf{k}+\mathbf{l}_{\pi^{-1}\circ\sigma}} - \delta_{\mathbf{l}_\pi,\mathbf{l}_\sigma}\delta_{\mathbf{k}_\pi,\mathbf{k}_\chi})\right| + \frac{1}{d^t}|M_{\mathbf{l},\mathbf{k}}|. \tag{49}$$

An upper bound of $|M_{\mathbf{l},\mathbf{k}}|$ can be obtained from the fact that the bases E and F are mutually unbiased, leading to

$$|M_{\mathbf{l},\mathbf{k}}| \leq \frac{1}{d^t} \sum_{\boldsymbol{\alpha}\in\mathcal{N}} |S_t \setminus S_t^{\boldsymbol{\alpha}}|. \tag{50}$$

As $|S_t\setminus S_t^{\boldsymbol{\alpha}}|$ depends only on how many different elements $\boldsymbol{\alpha}$ contains, the number of which we denote by k, and the number of every different element α_i in $\boldsymbol{\alpha}$, denoted by s_i, we replace the summation over $\boldsymbol{\alpha} \in \mathcal{N}$ with that over k and obtain

$$\sum_{\boldsymbol{\alpha}\in\mathcal{N}} |S_t \setminus S_t^{\boldsymbol{\alpha}}| = \sum_{k=1}^{t} \binom{d}{k} g^{(k)}(t), \tag{51}$$

where the binomial coefficient counts the number of possible choices of k different numbers from $[0, d-1]$, and $g^{(k)}(t)$ is the function that depends only on k and t given by

$$g^{(k)}(t) = \sum_{(s_1,\ldots,s_k)} \frac{t!}{s_1!\ldots s_k!} \left(t! - \frac{t!}{s_1!\ldots s_k!}\right). \tag{52}$$

Here, the summation is taken over all possible $(s_1, \ldots, s_k)$ such that $\forall i \in [1, k]$ $s_i \in [1, t]$ and $\sum_{i=1}^k s_i = t$. For a fixed k, the number of such combinations is simply given by

$\binom{t-1}{k-1}$. For $k=t$, $s_i=1$ for all $i\in[1,k]$, and, thus, $g^{(t)}(t)=0$. For the remaining terms $g^{(k)}(t)$ ($k\in[1,t-1]$), we use an upper bound given by

$$g^{(k)}(t)\le\binom{t-1}{k-1}\frac{t!^2}{4}, \tag{53}$$

which is optimal when $k=t-1$. Substituting these, we obtain

$$\sum_{\boldsymbol{\alpha}\in\mathcal{N}}|S_t\backslash S_t^{\boldsymbol{\alpha}}|\le\frac{t!^2}{4}\sum_{k=1}^{t-1}\binom{d}{k}\binom{t-1}{k-1} \tag{54}$$

$$=\frac{t!^2}{4}\left[\binom{d-1+t}{t}-\binom{d}{t}\right], \tag{55}$$

where the last line is obtained due to Vandermonde's identity. Since $d=\Omega(t^2)$, an upper bound is obtained such as

$$\sum_{\boldsymbol{\alpha}\in\mathcal{N}}|S_t\backslash S_t^{\boldsymbol{\alpha}}|\le t^2t!d^{t-1}+O(t^4t!d^{t-2}), \tag{56}$$

which leads to

$$\begin{aligned}&|\langle\mathbf{l},\mathbf{l}_\sigma^*|P_F-\sum_{\pi\in S_t}\Psi_\pi|\mathbf{k},\mathbf{k}_\chi^*\rangle|\\&\le\frac{1}{d^t}\left|\sum_{\pi\in S_t}(\delta_{\mathbf{l}+\mathbf{k}_{\pi^{-1}\circ\chi},\mathbf{k}+\mathbf{l}_{\pi^{-1}\circ\sigma}}-\delta_{\mathbf{l}_\pi,\mathbf{l}_\sigma}\delta_{\mathbf{k}_\pi,\mathbf{k}_\chi})\right|\\&\quad+\frac{t^2t!}{d^{t+1}}+O\left(\frac{t^4t!}{d^{t+2}}\right).\end{aligned} \tag{57}$$

Substituting this into C, the following upper bound can be obtained:

$$C\le\frac{t^2(t!^2+1)}{d}+\frac{1}{d^t}\max_{\mathbf{l}\in\mathcal{N}}\max_{\sigma\in S_t^{\mathbf{l}}}\sum_{\mathbf{k}\in\mathcal{N}}\sum_{\chi\in S_t^{\mathbf{k}}}\left|\sum_{\pi\in S_t}(\delta_{\mathbf{l}+\mathbf{k}_{\pi^{-1}\circ\chi},\mathbf{k}+\mathbf{l}_{\pi^{-1}\circ\sigma}}-\delta_{\mathbf{l}_\pi,\mathbf{l}_\sigma}\delta_{\mathbf{k}_\pi,\mathbf{k}_\chi})\right|+O\left(\frac{t^4t!^2}{d^2}\right) \tag{58}$$

$$=\frac{t^2(t!^2+1)}{d}+\frac{1}{d^t}\max_{\mathbf{l}\in\mathcal{N}}\max_{\sigma\in S_t^{\mathbf{l}}}\sum_{\mathbf{k}\in\mathcal{N}}\sum_{\chi\in S_t^{\mathbf{k}}}\sum_{\pi\in S_t}(\delta_{\mathbf{l}+\mathbf{k}_{\pi^{-1}\circ\chi},\mathbf{k}+\mathbf{l}_{\pi^{-1}\circ\sigma}}-\delta_{\mathbf{l}_\pi,\mathbf{l}_\sigma}\delta_{\mathbf{k}_\pi,\mathbf{k}_\chi})+O\left(\frac{t^4t!^2}{d^2}\right) \tag{59}$$

$$\le\frac{t^2(t!^2+1)}{d}+\frac{1}{d^t}\max_{\mathbf{l}\in\mathcal{N}}\max_{\sigma\in S_t^{\mathbf{l}}}\sum_{\pi\in S_t}\sum_{\mathbf{k}\in\mathcal{N}}\sum_{\chi(\neq\pi)\in S_t^{\mathbf{k}}}\delta_{\mathbf{l}+\mathbf{k}_{\pi^{-1}\circ\chi},\mathbf{k}+\mathbf{l}_{\pi^{-1}\circ\sigma}}+O\left(\frac{t^4t!^2}{d^2}\right) \tag{60}$$

$$\le\frac{t^2(t!^2+1)}{d}+\frac{1}{d^t}\max_{\mathbf{l}\in\mathcal{N}}\max_{\sigma\in S_t^{\mathbf{l}}}\sum_{\pi\in S_t}\sum_{\chi(\neq\pi)\in S_t}\sum_{\mathbf{k}\in\mathcal{N}}\delta_{\mathbf{l}+\mathbf{k}_{\pi^{-1}\circ\chi},\mathbf{k}+\mathbf{l}_{\pi^{-1}\circ\sigma}}+O\left(\frac{t^4t!^2}{d^2}\right), \tag{61}$$

where the second line is due to a fact that the term in the modulus is non-negative because, when the second term is one, the first term is also one, the third line is obtained by using a fact that the first and the second terms cancel each other when $\chi=\pi$ and by dropping negative terms when $\chi\neq\pi$, and the last line is due to $S_t^{\mathbf{k}}\subset S_t$. For the delta function $\delta_{\mathbf{l}+\mathbf{k}_{\pi^{-1}\circ\chi},\mathbf{k}+\mathbf{l}_{\pi^{-1}\circ\sigma}}$, we have

$$\begin{aligned}&\delta_{\mathbf{l}+\mathbf{k}_{\pi^{-1}\circ\chi},\mathbf{k}+\mathbf{l}_{\pi^{-1}\circ\sigma}}=1\\&\quad\Leftrightarrow\forall s\in[1,t],\qquad l_s+k_{\chi^{-1}\circ\pi(s)}=k_s+l_{\sigma^{-1}\circ\pi(s)}.\end{aligned} \tag{62}$$

When $\chi\neq\pi$, there exists at least one pair (s,s') ($s\neq s'\in[1,t]$) such that $\pi(s)=\chi(s')$. Hence, $k_{s'}=k_s+l_{\sigma^{-1}\circ\pi(s)}-l_s$ should be at least satisfied for the delta function to be nonzero. Thus, the number of $\mathbf{k}$ for which the delta function is nonzero is at most d^{t-1}. Based on this observation, we obtain

$$\max_{\mathbf{l}\in\mathcal{N}}\max_{\sigma\in S_t^{\mathbf{l}}}\sum_{\pi\in S_t}\sum_{\chi(\neq\pi)\in S_t}\sum_{\mathbf{k}\in\mathcal{N}}\delta_{\mathbf{l}+\mathbf{k}_{\pi^{-1}\circ\chi},\mathbf{k}+\mathbf{l}_{\pi^{-1}\circ\sigma}}\le t!^2d^{t-1}. \tag{63}$$

Substituting this into Eq. (61), we obtain an upper bound of C, leading to

$$\begin{aligned}&\|\mathbb{E}[(D^ED^FD'^E)^{\otimes t,t}]-\mathbb{E}[U^{\otimes t,t}]\|_\infty\\&\le\frac{(1+t^2)t!^2+t^2}{d}+O\left(\frac{t^4t!^2}{d^2}\right).\end{aligned} \tag{64}$$

This concludes the proof. ∎

C. Proof of the second main result

Here, we prove that $\Lambda_2=|L_2|\le 2^{2t^2+(t-1)N}$ for the 2-local permutation check problem, which is the key to obtaining Theorem 4. Here, L_2 is the set of pairs (K,K'), where K is a 2-local but not a row permutation of K'.

Throughout the proof, we denote the column vectors of K and K' by $\vec{k}_i$ and $\vec{k}'_i$, respectively, for $i\in[1,N]$. The

2-local permutation condition is equivalent to the following:

$$\forall i,j \in [1,N], \qquad \vec{k}_i \cdot \vec{k}_j = \vec{k}'_i \cdot \vec{k}'_j, \tag{65}$$

where the center dot $(\cdot)$ is the usual Euclidean inner product. This is because the conditions for $i = j$ imply that the number of 1's in $\vec{k}_i$ and that in $\vec{k}'_i$ should be the same, and those for $i \neq j$ imply that the number of 11 in $K_{\{i,j\}}$ is equal to that in $K'_{\{i,j\}}$. These conditions together correspond to the necessary and sufficient conditions for the pair (K, K') to be 2-local permutations. Moreover, Eq. (65) implies that the Gram matrix of a set $\{\vec{k}_i : i \in [1,N]\}$ of column vectors is the same as that of $\{\vec{k}'_i : i \in [1,N]\}$. Hence, $\mathrm{span}\{\vec{k}_i : i \in [1,N]\}$ has the same dimension as $\mathrm{span}\{\vec{k}'_i : i \in [1,N]\}$, and there exists a partial isometry O that satisfies $O\vec{k}_i = \vec{k}'_i$ for any $i \in [1,N]$, i.e., $OK = K'$. If the partial isometry is restricted to its support, it is an orthogonal matrix as the elements of the vectors are in $\{0,1\}$, and it is not a permutation operator due to the assumption that K is not a row permutation of K'.

We now construct a set $\mathcal{O}$ of orthogonal matrices on $\mathbb{R}^t$ that satisfies

$$\forall\ (K,K') \in L_2, \exists O \in \mathcal{O}, \quad \text{such that } OK = K'. \tag{66}$$

This can be done as follows. Let $s := 2^{2t}$ and $[0, s-1]^{\leq t}$ be the set of s-ary strings of length t or smaller. We describe a procedure of defining a set $S_2 \subset [0, s-1]^{\leq t}$ and orthogonal matrices $O_{\mathbf{b}}$ for $\mathbf{b} \in S_2$, such that S_2 is a prefix code and that $\mathcal{O} := \{O_{\mathbf{b}} | \mathbf{b} \in S_2\}$ satisfies Eq. (66). Our construction starts with $S_2 = \emptyset$ and is recursive in terms of the rank κ of the partial isometry obtained from (K, K'). We repeat the subroutine described below from $\kappa = t$ to $\kappa = 1$ by decreasing κ one by one. In the subroutine, we first choose $(K, K') \in L_2$ that defines a partial isometry with rank κ. We pick up an arbitrary set of independent column vectors $\{\vec{k}_{i_m}\}_{m=1}^{\kappa}$ in K and those $\{\vec{k}'_{i_m}\}_{m=1}^{\kappa}$ in K'. These vectors can be converted to an s-ary string $\mathbf{b} = (2^t k_{i_1} + k'_{i_1}, 2^t k_{i_2} + k'_{i_2}, \ldots, 2^t k_{i_\kappa} + k'_{i_\kappa})$ of length κ by regarding each vector as a binary number with length t. If $\mathbf{b}$ is a prefix of a string $\mathbf{b}' \in S_2$, then the orthogonal matrix $O_{\mathbf{b}'}$ satisfies $O_{\mathbf{b}'} K = K'$ because, on the support of the partial isometry obtained from (K, K'), the action of $O_{\mathbf{b}'}$ is the same as that of the isometry by construction. Otherwise, we append $\mathbf{b}$ to S_2 and define an orthogonal matrix $O_{\mathbf{b}}$ as an arbitrary extension of the partial isometry. The subroutine is run for all $(K, K') \in L_2$ with a partial isometry of rank κ. Eventually, we obtain a set $\mathcal{O}$ of orthogonal matrices on $\mathbb{R}^t$. Importantly, it does not contain a permutation matrix and, by construction, $|\mathcal{O}| = |S_2| \leq 2^{2t^2}$.

Introducing a set $L_2(O)$ by $\{(K, OK) : K, OK \in \{0,1\}^{tN}\}$ for a given orthogonal matrix $O \in \mathbb{R}^t$, we have $L_2 \subset \cup_{O \in \mathcal{O}} L_2(O)$, leading to

$$\Lambda_2 \leq \sum_{O \in \mathcal{O}} |L_2(O)| \tag{67}$$

$$\leq |\mathcal{O}| \max_{O \in \mathcal{O}} |L_2(O)| \tag{68}$$

$$\leq 2^{2t^2} \max_{O \in \mathcal{O}} |L_2(O)|. \tag{69}$$

Since the condition $OK \in \{0,1\}^{tN}$ consists of an identical and independent condition on each column of K, $|L_2(O)|$ for $O \in \mathcal{O}$ is bounded from above by

$$|L_2(O)| \leq (\max_{O \in \mathcal{O}} |\{\vec{k} \in \{0,1\}^t : O\vec{k} \in \{0,1\}^t\}|)^N. \tag{70}$$

To obtain an upper bound on the right-hand side, we use the following fact: let O be an orthogonal matrix acting on the Euclidean space $\mathbb{R}^t$, which contains the set of apexes of a hypercube, $\{0,1\}^t$. If there exists a set $S \subset \{0,1\}^t$ such that $OS \subset \{0,1\}^t$ and $|S| > 2^{t-1}$, then O is a permutation matrix. This is considered to be a type of constrained problems in extremal algebraic theory [62,63], and the proof is given in Appendix D. As $O \in \mathcal{O}$ is on $\mathbb{R}^t$ and is not a permutation matrix, we obtain

$$\max_{O \in \mathcal{O}} |\{\vec{k} \in \{0,1\}^t : O\vec{k} \in \{0,1\}^t| \leq 2^{t-1}. \tag{71}$$

Thus, we have $\Lambda_2 \leq 2^{2t^2 + (t-1)N}$. ∎

Finally, we note that the upper bound of Λ_2 is unlikely to be tight in terms of t because $|\mathcal{O}| \leq 2^{2t^2}$ in the proof is far from optimal. This is observed from the fact that $|\mathcal{O}| = |S_2|$ but S_2 does not contain all strings with length t. To be more concrete, we provide instances for a small t. From the result in Ref. [61], we know that, for any pair (K, K'), K is a row permutation of K' if and only if K is a $(\lfloor \log_2 t \rfloor + 1)$-local permutation of K'. Hence, the smallest t making the 2-local permutation check problem nontrivial is 4. In this case, we can show that if K is a 2-local but not a row permutation of K', the four rows of K and those of K' can be rearranged independently, resulting in K_π and K'_σ, respectively $(\pi, \sigma \in S_4)$, such that a pair of the ith column of K_π and that of K'_σ are in the set $C_0 \cup C_1$ $(\forall i \in [1,N])$, where

$$\begin{aligned} C_0 = \{&[(0,0,0,0)^T, (0,0,0,0)^T], [(1,1,1,1)^T, (1,1,1,1)^T] \\ &[(0,0,1,1)^T, (0,0,1,1)^T], [(1,1,0,0)^T, (1,1,0,0)^T] \\ &[(1,0,1,0)^T, (1,0,1,0)^T], [(0,1,0,1)^T, (0,1,0,1)^T]\}, \end{aligned} \tag{72}$$

$$C_1 = \{[(0,1,1,0)^T, (1,0,0,1)^T], [(1,0,0,1)^T, (0,1,1,0)^T]\}. \tag{73}$$

Taking the number of choices of π and σ into account, we have

$$\Lambda_2 < t!^2(|C_0| + |C_1|)^N = t!^2 8^N, \tag{74}$$

which corresponds to $t!^2 2^{(t-1)N}$ for $t = 4$. For this reason, we conjecture that the optimal bound should be given by $f(t)2^{(t-1)N}$, where $f(t) = O(\mathrm{poly}(t!))$, which we analytically confirm for $t \leq 7$. If this conjecture is true, Theorem 4 works for $t = o(N/\log N)$ instead of $t = o(N^{1/2})$.

D. Proof of the third main result

We prove Corollary 5 that, $\forall\, T \geq [2t + 1 + (2/N)\log(1/\epsilon)]\pi$, a random unitary $U_{XZ}(T) = \mathcal{T}\exp[-i\int_0^T ds H_{XZ}(s)]$ generated by $H_{XZ}(T) \in_R \mathfrak{H}_{XZ}^{(t)}$ at time T is an ϵ-approximate unitary t-design, where $\mathfrak{H}_{XZ}^{(t)}$ is the set of Hamiltonians in the form of Eq. (21).

In the proof, we denote $e^{-i\tau H_W^{(m)}}$ by $U_W^{(m)}(\tau)$ $(W = X, Z)$. As both Hamiltonians are composed of commuting terms, they are simply given by

$$e^{-i\tau H_X^{(m)}} = \prod_{k<k'} e^{i\tau J_{kk'}^{(m)} X_k \otimes X_{k'}} \prod_k e^{i\tau B_k^{(m)} X_k}, \tag{75}$$

$$e^{-i\tau H_Z^{(m)}} = \prod_{k<k'} e^{i\tau \tilde{J}_{kk'}^{(m)} Z_k \otimes Z_{k'}} \prod_k e^{i\tau \tilde{B}_k^{(m)} Z_k}. \tag{76}$$

We first consider a random unitary $U_{XZ}(T_\ell)$ at time $T_\ell = (2\ell + 1)\pi$ $(\ell = 1, 2, \ldots)$. Using the above notation, it is given by

$$U_{XZ}(T_\ell) = U_Z^{(\ell+1)}(\pi) \prod_{m=\ell}^{1} U_X^{(m)}(\pi) U_Z^{(m)}(\pi). \tag{77}$$

We take the average of $U_{XZ}(T_\ell)^{\otimes t,t}$ over $H_{XZ} \in_R \mathfrak{H}_{XZ}^{(t)}$, which is equivalent to taking the average over all parameters $B_k^{(m)}, \tilde{B}_{k'}^{(m)} \in_R \mathcal{P}_t(B)$ and $J_{kk'}^{(m)}, \tilde{J}_{kk'}^{(m)} \in_R \mathcal{P}_t(J)$. Here, the parameter set $\mathcal{P}_t(c)$ is given by Eq. (18), such as

$$\mathcal{P}_t(c) = \left\{ \frac{m}{2(\lfloor t/2 \rfloor + 1)} : m \in [-c, c] \right\}, \tag{78}$$

and $(B, J) = (\lfloor t/2 \rfloor + 1/2, \lfloor t/2 \rfloor/2)$. Since it holds that

$$\begin{aligned} &e^{i\pi J_{kk'}^{(m)} Z_k \otimes Z_{k'}} e^{i\pi B_k^{(m)} Z_k} \otimes e^{i\pi B_{k'}^{(m)} Z_{k'}} \\ &= e^{\pi i (J_{kk'}^{(m)} + B_k^{(m)} + B_{k'}^{(m)})} (\mathrm{diag}_Z\{1, e^{-2\pi i (J_{kk'}^{(m)} + B_{k'}^{(m)})}\} \\ &\quad \otimes \mathrm{diag}_Z\{1, e^{-2\pi i (J_{kk'}^{(m)} + B_k^{(m)})}\}) \mathrm{diag}_Z\{1, 1, 1, e^{4\pi i J_{kk'}^{(m)}}\}, \end{aligned} \tag{79}$$

if $B_k^{(m)}$, $B_{k'}^{(m)} \in_R \mathcal{B}_t$ and $J_{kk'}^{(m)} \in_R \mathcal{J}_t$, where

$$\mathcal{B}_t = \left\{ \frac{m}{2(\lfloor t/2 \rfloor + 1)} : m \in [0, 2\lfloor t/2 \rfloor + 1] \right\}, \tag{80}$$

$$\mathcal{J}_t = \left\{ \frac{m}{2(\lfloor t/2 \rfloor + 1)} : m \in [0, \lfloor t/2 \rfloor] \right\}, \tag{81}$$

then the probability distribution of $[-2\pi(J_{kk'}^{(m)} + B_{k'}), -2\pi(J_{kk'}^{(m)} + B_k^{(m)}), 4\pi J_{kk'}^{(m)}]$ is identical to that of $(\varphi, \varphi', \theta)$ in Eq. (14) with $a = 2(\lfloor t/2 \rfloor + 1)$ and $b = \lfloor t/2 \rfloor + 1$, implying that $U_Z^{(m)}(T_\ell)$ is equivalent to $\mathrm{RDC}_{\mathrm{disc}}(\mathcal{I}_2 : 2b, b)$ up to a global phase. Noting that the global phase is canceled in $U_Z^{(m)}(T_\ell)^{\otimes t,t}$ and recalling that $\mathbb{E}[\mathrm{RDC}_{\mathrm{disc}}(\mathcal{I}_2 : a, b)^{\otimes t,t}] = \mathbb{E}[\mathrm{RDC}(\mathcal{I}_2)^{\otimes t,t}]$ if $a \geq t + 1$ and $b \geq \lfloor t/2 \rfloor + 1$, we have

$$\mathbb{E}_{B_k^{(m)} \in_R \mathcal{B}_t, J_{kk'}^{(m)} \in_R \mathcal{J}_t} [U_Z^{(m)}(T_\ell)^{\otimes t,t}] = \mathbb{E}[\mathrm{RDC}(\mathcal{I}_2)^{\otimes t,t}]. \tag{82}$$

Using a product of two-qubit diagonal gates V given by

$$V = \bigotimes_{k=1}^{N} \mathrm{diag}_Z^{(k)}\{1, e^{2\pi i \Delta B}\} \bigotimes_{k<k'} \mathrm{diag}_Z^{(kk')}\{1, 1, 1, e^{-4\pi i \Delta J}\}, \tag{83}$$

where the superscript of diag_Z, such as (k) and (kk'), indicates the place of qubits the gate acts on, $2\Delta B = (\lfloor t/2 \rfloor + 1/2)/(\lfloor t/2 \rfloor + 1)$, and $4\Delta J = \lfloor t/2 \rfloor/(\lfloor t/2 \rfloor + 1)$, we obtain

$$\begin{aligned} &\mathbb{E}_{B_k^{(m)} \in_R \mathcal{P}_t(B), J_{kk'}^{(m)} \in_R \mathcal{P}_t(J)} [U_Z^{(m)}(T_\ell)^{\otimes t,t}] \\ &= \mathbb{E}_{B_k^{(m)} \in_R \mathcal{B}_t, J_{kk'}^{(m)} \in_R \mathcal{J}_t} [U_Z^{(m)}(T_\ell)^{\otimes t,t}] V^{\otimes t,t} \qquad (84) \\ &= \mathbb{E}[\mathrm{RDC}(\mathcal{I}_2)^{\otimes t,t}] V^{\otimes t,t}, \qquad (85) \end{aligned}$$

where we use Eq. (82) in the last line. Further, because $\mathrm{RDC}(\mathcal{I}_2)$ is composed of two-qubit diagonal gates with random phases uniformly drawn from $[0, 2\pi)$, the average of $\mathrm{RDC}(\mathcal{I}_2)^{\otimes t,t}$ does not change even when additional diagonal two-qubit gates, such as V, are applied. Thus, we obtain

$$\mathbb{E}_{B_k^{(m)} \in_R \mathcal{P}_t(B), J_{kk'}^{(m)} \in_R \mathcal{P}_t(J)} [U_Z^{(m)}(T_\ell)^{\otimes t,t}] = \mathbb{E}[\mathrm{RDC}(\mathcal{I}_2)^{\otimes t,t}]. \tag{86}$$

As a similar relation holds for X Hamiltonians, we conclude that

$$\mathbb{E}[U_{XZ}(T_\ell)^{\otimes t,t}] = \mathbb{E}\{[(\mathrm{RDC}(\mathcal{I}_2) H_N)^{2\ell} \mathrm{RDC}(\mathcal{I}_2)]^{\otimes t,t}\}, \tag{87}$$

where H_N is the Hadamard transformation on N qubits, implying that $U_{XZ}(T_\ell)$ is an ϵ-approximate unitary t-design if $\ell \geq t + (1/N)\log_2(1/\epsilon)$.

To complete the proof, consider the time T satisfying $T_\ell < T < T_{\ell+1}$, where $\ell \geq t + (1/N)\log_2(1/\epsilon)$. Because the time-evolution operator from time T_ℓ to time T is independent of the one before T_ℓ, $U_{XZ}(T)$ is also an ϵ-approximate unitary t-design. ∎

V. CONCLUSION AND DISCUSSION

In this paper, we present new constructions of unitary t-designs and propose design Hamiltonians as a general framework to investigate randomizing operations in complex quantum many-body systems. The new constructions are based on repetitions of random diagonal unitaries in mutually unbiased bases. We first show that, if the bases are Fourier-type, approximate unitary t-designs can be achieved on one qudit after $O(t)$ repetitions. We then constructed quantum circuits on N qubits that achieve approximate unitary t-designs using $O(tN^2)$ gates, which drastically improves the previous result [35,43] in terms of t. The dependence on t is essentially optimal among designs with finite supports. The circuits are obtained by solving a special case of combinatorial problems, which we call the local permutation check problems, showing an interesting connection between combinatorics and efficient implementations of designs. Based on these results, we provide a design Hamiltonian, which changes the interactions only a few times to generate designs. This result supports the natural design Hamiltonian conjecture and is also practically important as it simplifies the experimental implementations of unitary designs.

Our approach of studying unitary designs and randomizing operations in physically natural systems opens a lot of interesting questions. The following are a few questions concerning unitary designs.

(1) In one-qudit systems, is it possible to implement unitary t-designs by repeating random diagonal unitaries in *any* nontrivial pairs of bases? If so, how many repetitions are sufficient for the implementations?

(2) What is the best strategy of the local permutation check problems?

(3) What is the most efficient implementation by quantum circuits that approximate random diagonal unitaries in the Pauli-Z basis?

(4) What are the further applications of unitary t-designs for $t \geq 4$?

Regarding question (1), we find that repeating random diagonal unitaries in nontrivial pairs of bases achieves a unitary 1-design if any vector in one basis is not orthogonal to any vector in the other basis. Although this nonorthogonality condition may not be necessary, we expect that, for arbitrary nontrivial pairs of bases satisfying the nonorthogonality condition, the process eventually achieves unitary t-designs. Questions (2) and (3) are related to each other. In this paper, we considered only 2-local permutation check problems. However, if there exists a set $\mathcal{I} = \{I\}$ such that $\Lambda(\mathcal{I}) = O(2^{(t-1)N})$ and $|I| = \text{const}$ for all $I \in \mathcal{I}$, then we can implement approximate unitary t-designs using $O(t|\mathcal{I}|)$ quantum gates. Hence, finding a better strategy for the local permutation check problems immediately results in a faster implementation of unitary designs. It is also desirable to directly search efficient quantum circuits approximating random diagonal unitaries in the Z basis. Finally, it is important to find applications of unitary t-designs for large t. A possible and promising direction is to further explore large deviation bounds for unitary designs, as mentioned in Sec. III B.

We also list a few open questions about design Hamiltonians from the physical point of view.

(I) Prove or disprove the natural design Hamiltonian conjecture.

(II) What are the exact relations between natural design Hamiltonians and various definitions of scrambling or OTO correlators?

(III) If a design Hamiltonian is defined on a finite ensemble of local Hamiltonians, how many Hamiltonians are needed?

(IV) What are the static features of design Hamiltonians such as thermal or quantum phases?

Question (I) is the most interesting one, where we could use the methods developed in the random matrix theory [80]. A natural candidate of design Hamiltonians satisfying all three conditions of the conjecture may be $H_{\text{local GUE}} = \sum_{\langle i,j\rangle} h_{ij}$, where each local term h_{ij} is drawn randomly and independently from the so-called Gaussian unitary ensemble [80] and the summation is taken over all neighboring qubits. We expect that $H_{\text{local GUE}}$ generates a unitary design after some time, although it may also be possible that it does not, due to the many-body localization. Question (II) is important to clarify the roles of design Hamiltonians in black hole information science and quantum chaos. As design Hamiltonians are based on unitary designs, it suffices to investigate explicit relations between unitary designs and scrambling or the OTO correlators. The relation between unitary designs and the OTO correlators has been addressed recently and is clarified in Ref. [76]. Question (III) is not only of theoretical interest but also of practical importance because it determines the number of random bits necessary to construct design Hamiltonians. To address this question, it is needed to relax the definition of design Hamiltonians to exclude the Poincaré recurrence time, as we mention in Sec. III C. Note that, since the support of unitary t-designs on N qubits should contain at least $O(2^{2tN})$ unitaries [64], the ensemble should contain at least the same number of Hamiltonians. Finally, as design Hamiltonians are certain types of disordered Hamiltonians, it is natural to expect that they have special static properties, which is question (IV). A static property of the above random Hamiltonian $H_{\text{local GUE}}$ was numerically studied from the viewpoint of distributions in a state space, and evidence of phase transitions was obtained [81]. However, as $H_{\text{local GUE}}$ is not yet shown to be a design Hamiltonian and no time-independent design Hamiltonians have been

found yet, it would be more realistic to start with investigating static properties of the Hamiltonian H_Z of H_{XZ}, which has similarity to many-body localized systems, and their dependence on t.

ACKNOWLEDGMENTS

The authors are grateful to S. Di Martino, C. Morgan, and T. Sasaki for helpful discussions. The authors also thank B. Yoshida for fruitful discussions and for telling us about recent progress on scrambling and quantum chaos, and C. Gogolin for pointing out the possibility of using our construction for quantum metrology. This work was supported by CREST, JST, Grant No. JPMJCR1671. Y. N. is a JSPS Research Fellow and is supported by JSPS KAKENHI Grant No. 272650. A. W. and C. H. are supported by the Spanish MINECO, Projects No. FIS2013-40627-P and No. FIS2016-80681-P, and C. H. by FPI Grant No. BES-2014-068888, as well as by the Generalitat de Catalunya, CIRIT Project No. 2014 SGR 966. A. W. is further supported by the European Commission (STREP "RAQUEL"), the European Research Council (Advanced Grant "IRQUAT").

APPENDIX A: PROOF OF THEOREM 1

Here, we provide a proof of Theorem 1, which follows almost directly from the simple fact that, for any unitary U, $U^{\otimes t,t} = P_0 + (I - P_0)U^{\otimes t,t}(I - P_0)$. This observation is obtained as follows: using $|\Psi_\pi\rangle = I \otimes V(\pi)|\Phi\rangle$, we have for any $\pi \in S_t$ that

$$U^{\otimes t,t}|\Psi_\pi\rangle = U^{\otimes t} \otimes U^{*\otimes t} V(\pi)|\Phi\rangle \tag{A1}$$

$$= U^{\otimes t} \otimes V(\pi) U^{*\otimes t}|\Phi\rangle \tag{A2}$$

$$= U^{\otimes t} U^{\dagger \otimes t} \otimes V(\pi)|\Phi\rangle \tag{A3}$$

$$= I \otimes V(\pi)|\Phi\rangle \tag{A4}$$

$$= |\Psi_\pi\rangle, \tag{A5}$$

where we use the fact that $U^{*\otimes t}$ commutes with $V(\pi)$ in the second line and the property of the maximally entangled state in the third line. This implies that $(I - P_0)U^{\otimes t,t}P_0 = 0$. Replacing U with $U^\dagger$ in Eq. (A5), we also have $(I - P_0)U^{\dagger\otimes t,t}P_0 = 0$, implying $P_0 U^{\otimes t,t}(I - P_0) = 0$. Hence, we obtain $U^{\otimes t,t} = P_0 + (I - P_0)U^{\otimes t,t}(I - P_0)$.

To prove Theorem 1, let ν be a quantum (η, t) TPE satisfying

$$\|\mathbb{E}_{U\sim\nu}[U^{\otimes t,t}] - \mathbb{E}_{U\sim \mathsf{H}}[U^{\otimes t,t}]\|_\infty \le \eta. \tag{A6}$$

Decomposing $U^{\otimes t,t}$ into $P_0 + (I - P_0)U^{\otimes t,t}(I - P_0)$, we have

$$\mathbb{E}_{U\sim\nu}[U^{\otimes t,t}] = P_0 + (I - P_0)\mathbb{E}_{U\sim\nu}[U^{\otimes t,t}](I - P_0). \tag{A7}$$

Because of Eq. (30), the quantum TPE ν satisfies that

$$\|(I - P_0)\mathbb{E}_{U\sim\nu}[U^{\otimes t,t}](I - P_0)\|_\infty \le \eta. \tag{A8}$$

Let ν^ℓ be a measure corresponding to that of the ℓ iterations of the quantum TPE ν. Then,

$$\|\mathcal{G}^{(t)}_{U\sim\nu^\ell} - \mathcal{G}^{(t)}_{U\sim \mathsf{H}}\|_\diamond \tag{A9}$$

$$\le d^t \|\mathcal{G}^{(t)}_{U\sim\nu^\ell} - \mathcal{G}^{(t)}_{U\sim \mathsf{H}}\|_{2\to 2} \tag{A10}$$

$$= d^t \|\mathbb{E}_{U\sim\nu^\ell}[U^{\otimes t,t}] - \mathbb{E}_{U\sim \mathsf{H}}[U^{\otimes t,t}]\|_\infty \tag{A11}$$

$$= d^t \|(\mathbb{E}_{U\sim\nu}[U^{\otimes t,t}])^\ell - \mathbb{E}_{U\sim \mathsf{H}}[U^{\otimes t,t}]\|_\infty \tag{A12}$$

$$= d^t \|[(I - P_0)\mathbb{E}_{U\sim\nu}[U^{\otimes t,t}](I - P_0)]^\ell\|_\infty \tag{A13}$$

$$\le d^t \|(I - P_0)\mathbb{E}_{U\sim\nu}[U^{\otimes t,t}](I - P_0)\|^\ell_\infty \tag{A14}$$

$$\le d^t \eta^\ell. \tag{A15}$$

Here, the second line is due to the inequality that $\|\mathcal{E}\|_\diamond \le D\|\mathcal{E}\|_{2\to 2}$ for any superoperators $\mathcal{E}$ acting on a D-dimensional system, the fourth line is obtained due to the independence of the measure of each iteration, the fifth line is from Eq. (A7), and the last line is from Eq. (A8). This implies that ℓ iterations of a quantum (η, t) TPE is an ϵ-approximate unitary t-design if $d^t\eta^\ell \le \epsilon$.

APPENDIX B: FOURIER-TYPE PAIRS OF BASES

Here, we show that a pair of arbitrary basis and its Fourier basis, and a pair of the Pauli-X and -Z bases are Fourier type.

When a pair of two bases is that of an arbitrary basis and its Fourier basis, it is clear that $\theta_{k\alpha} = (2\pi k\alpha/d)$ and the additive operation in the index is given by an addition modulo d. It is also obvious that $[0, d-1]$ is an additive group with respect to the modular addition.

When the pair is given by the Pauli-X and -Z bases, using the binary representation such as $\alpha = \alpha_1 \ldots \alpha_N$ $(\forall j \in [1, N], \alpha_j \in \{0, 1\})$, the Pauli-$X$ and -Z bases can be represented by

$$|\alpha\rangle_X = \bigotimes_{j=1}^N |\alpha_j\rangle_X, \qquad |k\rangle_Z = \bigotimes_{j=1}^N |k_j\rangle_Z, \tag{B1}$$

respectively. Using the fact that ${}_Z\langle k_j|\alpha_j\rangle_X = {}_X\langle\alpha_j|k_j\rangle_Z$ is equal to $1/\sqrt{2}$ if $(\alpha_j, k_j) = (0,0), (0,1), (1,0)$ and is equal to $-1/\sqrt{2}$ if $(\alpha_j, k_j) = (1,1)$, we have $\theta_{k\alpha} = \pi \sum_{j=1}^N \delta_{k_j 1}\delta_{\alpha_j 1}$, leading to

$$\exp[i(\theta_{k\alpha}+\theta_{l\alpha})]=\exp\left[i\pi\sum_{j=1}^{N}(\delta_{k_j1}+\delta_{l_j1})\delta_{\alpha_j1}\right] \tag{B2}$$

$$=\exp\left[i\pi\sum_{j=1}^{N}\delta_{k_j+l_j,1}\delta_{\alpha_j1}\right] \tag{B3}$$

$$=\exp[i\theta_{k\oplus l,\alpha}], \tag{B4}$$

where $\oplus$ is a bitwise XOR, defined by $a\oplus b=0$ when $a=b$ and otherwise 1 for binary numbers a and b, and is the additive operation.

APPENDIX C: LOCAL PERMUTATION CHECK PROBLEMS AND THE ACHIEVABILITY OF QUANTUM TPE

Here, we show how the achievability of quantum TPE with a random diagonal circuit $\mathrm{RDC}(\mathcal{I})$ is connected to the $\mathcal{I}$-local permutation check problem.

Let $\mathsf{RDC}(\mathcal{I})$ be the probability measure of $\mathrm{RDC}(\mathcal{I})$. We denote the averaged operators $\mathbb{E}_{D^Z\sim\mathsf{RDC}(\mathcal{I})}[(D^Z)^{\otimes t,t}]$ and $\mathbb{E}_{D^Z\sim\mathsf{D}_Z}[(D^Z)^{\otimes t,t}]$ by Q_Z and P_Z, respectively. There exists a projector R_Z diagonal in the Pauli-Z basis such that $Q_Z=P_Z+R_Z$ because $Q_ZP_Z=P_ZQ_Z=P_Z$ and Q_Z is a projector diagonal in the Pauli-Z basis. Denoting $H_N^{\otimes t,t}Q_ZH_N^{\otimes t,t}$ by Q_X, where $H_N:=H^{\otimes N}$ is the Hadamard transformation on N qubits, and similarly decomposing it into P_X+R_X ($P_X:=H_N^{\otimes t,t}P_ZH_N^{\otimes t,t}$ and $R_X:=H_N^{\otimes t,t}R_ZH_N^{\otimes t,t}$), we have

$$\|Q_ZQ_XQ_Z-P_0\|_\infty=\|P_ZP_XP_Z-P_0+R_ZP_XP_Z+Q_ZP_XR_Z+Q_ZR_XP_Z+Q_ZR_XR_Z\|_\infty \tag{C1}$$

$$\le\|P_ZP_XP_Z-P_0\|_\infty+2\|P_XR_Z\|_\infty+\|R_XP_Z\|_\infty+\|R_XR_Z\|_\infty \tag{C2}$$

$$\le\eta+2\|P_XR_Z\|_\infty+\|R_XP_Z\|_\infty+\|R_XR_Z\|_\infty, \tag{C3}$$

where we use Theorem 2 in the last line.

We denote by $\mathcal{W}_Z$ a set of $(\mathbf{k}_1,\mathbf{k}_2)\in\mathcal{N}\times\mathcal{N}$ such that $\langle\mathbf{k}_1,\mathbf{k}_2|R_Z|\mathbf{k}_1,\mathbf{k}_2\rangle=1$. Using an upper bound of the operator norm by the row norm and using the fact that $|\langle\mathbf{l}_1,\mathbf{l}_2|P_X|\mathbf{k}_1,\mathbf{k}_2\rangle|=(\mathrm{tr}P_X)/2^{2tN}\le t!/2^{tN}$ for any $(\mathbf{k}_1,\mathbf{k}_2)$ and $(\mathbf{l}_1,\mathbf{l}_2)$, we obtain

$$\|R_XP_Z\|_\infty=\|P_XR_Z\|_\infty \tag{C4}$$

$$\le\max_{(\mathbf{l}_1,\mathbf{l}_2)\in\mathcal{W}_Z}\sum_{(\mathbf{k}_1,\mathbf{k}_2)\in\mathcal{W}_Z}|\langle\mathbf{l}_1,\mathbf{l}_2|P_X|\mathbf{k}_1,\mathbf{k}_2\rangle| \tag{C5}$$

$$\le\frac{t!}{2^{tN}}|\mathcal{W}_Z|. \tag{C6}$$

Similarly, we have

$$\|R_XR_Z\|_\infty\le\max_{(\mathbf{l}_1,\mathbf{l}_2)\in\mathcal{W}_Z}\sum_{(\mathbf{k}_1,\mathbf{k}_2)\in\mathcal{W}_Z}|\langle\mathbf{l}_1,\mathbf{l}_2|R_X|\mathbf{k}_1,\mathbf{k}_2\rangle| \tag{C7}$$

$$\le\left(\frac{|\mathcal{W}_Z|}{2^{tN}}\right)^2. \tag{C8}$$

Substituting Eqs. (C6) and (C8) into Eq. (C3), we obtain

$$\|Q_ZQ_XQ_Z-P_0\|_\infty\le\eta+3t!\frac{|\mathcal{W}_Z|}{2^{tN}}+\left(\frac{|\mathcal{W}_Z|}{2^{tN}}\right)^2. \tag{C9}$$

We finally show that $|\mathcal{W}_Z|=\Lambda(\mathcal{I})$. Note that $\Lambda(\mathcal{I})$ is the number of $(K,K')\in\{0,1\}^{tN}\times\{0,1\}^{tN}$ such that K is not a row permutation but is an $\mathcal{I}$-local permutation of K'. We first express each $k_s\in\mathbf{k}$ in binary, such as $k_s=k_{s1}\ldots k_{sN}$, and define a $t\times N$ matrix K with elements in $\{0,1\}$ corresponding to $\mathbf{k}$:

$$K:=\begin{pmatrix}k_{11}&k_{12}&\cdots&k_{1N}\\ \vdots&\vdots&\ddots&\vdots\\ k_{t1}&k_{t2}&\cdots&k_{tN}\end{pmatrix}, \tag{C10}$$

where $k_{sm}\in\{0,1\}$. Using this notation and noting that the Z basis is real, the state $|\mathbf{k},\mathbf{k}'^*\rangle$ is expressed as $|K,K'\rangle$. A random diagonal gate in $\mathrm{RDC}(\mathcal{I})$ applied on qubits in $I\in\mathcal{I}$ corresponds to, after taking the tensor product and the average, a projector onto $\mathrm{span}\{|K,K'\rangle:\Omega(K_I)=\Omega(K'_I)\}$, where Ω is a canonical map that rearranges $|I|$-bit sequences $\{K_{s,I}\}_{s\in[1,t]}$ in ascending order. Thus, we have

$$\langle K,K'|Q_Z|K,K'\rangle=\begin{cases}1 & \text{if } \forall\ I\in\mathcal{I},\Omega(K_I)=\Omega(K'_I)\\ 0 & \text{otherwise}\end{cases}. \tag{C11}$$

Note that the off-diagonal elements of Q_Z are always zero because it is diagonal in the Z basis. We also have

$$\langle K, K'|P_Z|K, K'\rangle = \begin{cases} 1 & \text{if } K \text{ is a row permutation of } K' \\ 0 & \text{otherwise.} \end{cases} \tag{C12}$$

From these two equations, it is clear that $R_Z = Q_Z - P_Z$ satisfies that $\langle K, K'|R_Z|K, K'\rangle = 1$ if and only if K is not a row permutation but is an $\mathcal{I}$-local permutation of K'. Otherwise, $\langle K, K'|R_Z|K, K'\rangle = 0$. This implies $|\mathcal{W}_Z| = \Lambda(\mathcal{I})$.

APPENDIX D: KEY STATEMENT IN THE PROOF OF THEOREM 4

Here, we prove the following statement, which is used in the proof of Theorem 4: let O be an orthogonal matrix acting on the Euclidean space $\mathbb{R}^t$, which contains a hypercube $\{0,1\}^t$. If there exists a set $S \subset \{0,1\}^t$ such that $OS \subset \{0,1\}^t$ and $|S| > 2^{t-1}$, then O is a permutation matrix.

Let $i \in [1,t]$ and $\vec{e}_i$ be a vector with elements in $\{0,1\}$, where only the ith element is 1:

$$\vec{e}_i = (0,\ldots,0,\overset{i}{\overbrace{1}},0,\ldots,0)^T. \tag{D1}$$

Then, for any i, there exists a vector $\vec{v}_i \in \{0,1\}^t$ such that both $\vec{v}_i$ and $\vec{v}_i + \vec{e}_i$ are contained in S. This is for the following reason: if there is no such pair of $\vec{v}_i$ and $\vec{v}_i + \vec{e}_i$, it implies that a pair of vectors, which have different values only at the ith element, is not contained in S. This results in $|S| \leq 2^{t-1}$, which is in contradiction to the assumption that $|S| > 2^{t-1}$.

As $\vec{v}_i + \vec{e}_i \in S \subset \{0,1\}^t$, the ith element of $\vec{v}_i$ is 0. Hence, we have $\vec{v}_i \cdot \vec{e}_i = 0$, implying that

$$O\vec{e}_i \cdot O(\vec{v}_i + \vec{e}_i) = \vec{e}_i \cdot \vec{v}_i + \vec{e}_i \cdot \vec{e}_i = \vec{e}_i \cdot \vec{e}_i = 1. \tag{D2}$$

It is also trivial that $O\vec{e}_i \cdot O\vec{e}_i = 1$ and that $O\vec{e}_i \in \{-1,0,1\}^t$, which follows from an identity $O\vec{e}_i = O(\vec{v}_i + \vec{e}_i) - O\vec{v}_i$ and the fact that both $O(\vec{v}_i + \vec{e}_i)$ and $O\vec{v}_i$ are in $\{0,1\}^t$. From these three relations and again $O(\vec{v}_i + \vec{e}_i) \in \{0,1\}^t$, we conclude that

$$O\vec{e}_i = \vec{e}_j = (0,\ldots,0,\overset{j}{\overbrace{1}},0,\ldots,0)^T \tag{D3}$$

for some $j \in [1,t]$. Because O is invertible, this implies that O is a permutation matrix.

[1] I. Devetak, *The Private Classical Capacity and Quantum Capacity of a Quantum Channel*, IEEE Trans. Inf. Theory **51**, 44 (2005).

[2] I. Devetak and A. Winter, *Relating Quantum Privacy and Quantum Coherence: An Operational Approach*, Phys. Rev. Lett. **93**, 080501 (2004).

[3] B. Groisman, S. Popescu, and A. Winter, *Quantum, Classical, and Total Amount of Correlations in a Quantum State*, Phys. Rev. A **72**, 032317 (2005).

[4] A. Abeyesinghe, I. Devetak, P. Hayden, and A. Winter, *The Mother of All Protocols: Restructuring Quantum Information's Family Tree*, Proc. R. Soc. A **465**, 2537 (2009).

[5] P. Hayden, *Quantum Information Theory via Decoupling*, http://qip2011.quantumlah.org/images/QIPtutorial1.pdf.

[6] F. Dupuis, M. Berta, J. Wullschleger, and R. Renner, *One-Shot Decoupling*, Commun. Math. Phys. **328**, 251 (2014).

[7] O. Szehr, F. Dupuis, M. Tomamichel, and R. Renner, *Decoupling with Unitary Approximate Two-Designs*, New J. Phys. **15**, 053022 (2013).

[8] C. Hirche and C. Morgan, in *Proceedings of the 2014 IEEE International Symposium on Information Theory* (IEEE, New York, 2014), p. 536.

[9] J. Emerson, R. Alicki, and K. Życzkowski, *Scalable Noise Estimation with Random Unitary Operators*, J. Opt. B **7**, S347 (2005).

[10] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland, *Randomized Benchmarking of Quantum Gates*, Phys. Rev. A **77**, 012307 (2008).

[11] E. Magesan, J. M. Gambetta, and J. Emerson, *Scalable and Robust Randomized Benchmarking of Quantum Processes*, Phys. Rev. Lett. **106**, 180504 (2011).

[12] E. Magesan, J. M. Gambetta, and J. Emerson, *Characterizing Quantum Gates via Randomized Benchmarking*, Phys. Rev. A **85**, 042311 (2012).

[13] P. Sen, *Random Measurement Bases, Quantum State Distinction and Applications to the Hidden Subgroup Problem*, arXiv:quant-ph/0512085.

[14] F. G. S. L. Brandão and M. Horodecki, *Exponential Quantum Speed-ups are Generic*, Quantum Inf. Comput. **13**, 0901 (2013).

[15] R. Kueng, H. Rauhut, and U. Terstiege, *Low Rank Matrix Recovery from Rank One Measurements*, arXiv:1410.6913.

[16] S. Kimmel and Y.-K. Liu, *Quantum Compressed Sensing Using 2-Designs*, arXiv:1510.08887.

[17] R. Kueng, H. Zhu, and D. Gross, *Distinguishing Quantum States Using Clifford Orbits*, arXiv:1609.08595.

[18] M. Oszmaniec, R. Augusiak, C. Gogolin, J. Kołodyński, A. Acín, and M. Lewenstein, *Random Bosonic States for Robust Quantum Metrology*, Phys. Rev. X **6**, 041044 (2016).

[19] S. Popescu, A. J. Short, and A. Winter, *Entanglement and the Foundations of Statistical Mechanics*, Nat. Phys. **2**, 754 (2006).

[20] S. Goldstein, J. L. Lebowitz, R. Tumulka, and N. Zanghí, *Canonical Typicality*, Phys. Rev. Lett. **96**, 050403 (2006).

[21] P. Reimann, *Foundation of Statistical Mechanics under Experimentally Realistic Conditions*, Phys. Rev. Lett. **101**, 190403 (2008).

[22] C. Gogolin and J. Eisert, *Equilibration, Thermalisation, and the Emergence of Statistical Mechanics in Closed Quantum Systems*, Rep. Prog. Phys. **79**, 056001 (2016).

[23] P. Hayden and J. Preskill, *Black Holes as Mirrors: Quantum Information in Random Subsystems*, J. High Energy Phys. 09 (2007) 120.

[24] Y. Sekino and L. Susskind, *Fast Scramblers*, J. High Energy Phys. 10 (2008) 065.

[25] L. Susskind, *Addendum to Fast Scramblers*, arXiv:1101.6048.

[26] N. Lashkari, D. Stanford, M. Hastings, T. Osborne, and P. Hayden, *Towards the Fast Scrambling Conjecture*, J. High Energy Phys. 04 (2013) 022.

[27] L. Susskind, *Computational Complexity and Black Hole Horizons*, arXiv:1402.5674.

[28] P. Hosur, X.-L. Qi, D. A. Roberts, and B. Yoshida, *Chaos in Quantum Channels*, J. High Energy Phys. 02 (2016) 04.

[29] H. Shenker and D. Stanfor, *Black Holes and the Butterfly Effect*, J. High Energy Phys. 03 (2014) 67.

[30] D. A. Roberts and D. Stanford, *Diagnosing Chaos Using Four-Point Functions in Two-Dimensional Conformal Field Theory*, Phys. Rev. Lett. **115**, 131603 (2015).

[31] S. H. Shenker and D. Stanford, *Stringy Effects in Scrambling*, J. High Energy Phys. 05 (2015) 132.

[32] A. Ambainis and A. Smith, in *Proceedings of RANDOM 2004* (Springer-Verlag, Berlin, Heidelberg, 2004), pp. 249–260.

[33] A. W. Harrow and R. A. Low, in *Proceedings of RANDOM 2009* (Springer-Verlag, Berlin, Heidelberg, 2009), pp. 548–561.

[34] A. W. Harrow and R. A. Low, *Random Quantum Circuits are Approximate 2-Designs*, Commun. Math. Phys. **291**, 257 (2009).

[35] F. G. S. L. Brandão, A. W. Harrow, and M. Horodecki, *Efficient Quantum Pseudorandomness*, Phys. Rev. Lett. **116**, 170502 (2016).

[36] D. P. DiVincenzo, D. W. Leung, and B. M. Terhal, *Quantum Data Hiding*, IEEE Trans. Inf. Theory **48**, 580 (2002).

[37] C. Dankert, R. Cleve, J. Emerson, and E. Livine, *Exact and Approximate Unitary 2-Designs and Their Application to Fidelity Estimation*, Phys. Rev. A **80**, 012304 (2009).

[38] D. Gross, K. Audenaert, and J. Eisert, *Evenly Distributed Unitaries: On the Structure of Unitary Designs*, J. Math. Phys. (N.Y.) **48**, 052104 (2007).

[39] G. Tóth and J. J. García-Ripoll, *Efficient Algorithm for Multiqudit Twirling for Ensemble Quantum Computation*, Phys. Rev. A **75**, 042311 (2007).

[40] W. G. Brown, Y. S. Weinstein, and L. Viola, *Quantum Pseudorandomness from Cluster-State Quantum Computation*, Phys. Rev. A **77**, 040303(R) (2008).

[41] Y. S. Weinstein, W. G. Brown, and L. Viola, *Parameters of Pseudorandom Quantum Circuits*, Phys. Rev. A **78**, 052332 (2008).

[42] I. T. Diniz and D. Jonathan, *Comment on "Random Quantum Circuits Are Approximate 2-Designs"*, Commun. Math. Phys. **304**, 281 (2011).

[43] F. G. S. L. Brandão, A. W. Harrow, and M. Horodecki, *Local Random Quantum Circuits Are Approximate Polynomial-Designs*, arXiv:1208.0692.

[44] R. Cleve, D. Leung, L. Liu, and C. Wang, *Near-Linear Constructions of Exact Unitary 2-Designs*, Quantum Inf. Comput. **16**, 0721 (2016).

[45] Y. Nakata, C. Hirche, C. Morgan, and A. Winter, *Unitary 2-Designs from Random X- and Z-Diagonal Unitaries*, arXiv:1502.07514.

[46] H. Zhu, *Multiqubit Clifford Groups Are Unitary 3-Designs*, arXiv:1510.02619.

[47] Z. Webb, *The Clifford Group Forms a Unitary 3-Design*, Quantum Inf. Comput. **16**, 1379 (2016).

[48] C. A. Ryan, M. Laforest, and R. Laflamme, *Randomized Benchmarking of Single- and Multi-Qubit Control in Liquid-State NMR Quantum Information Processing*, New J. Phys. **11**, 013034 (2009).

[49] K. R. Brown, A. C. Wilson, Y. Colombe, C. Ospelkaus, A. M. Meier, E. Knill, D. Leibfried, and D. J. Wineland, *Single-Qubit-Gate Error Below* 10^{-4} *in a Trapped Ion*, Phys. Rev. A **84**, 030303 (2011).

[50] A. D. Córcoles, J. M. Gambetta, J. M. Chow, J. A. Smolin, M. Ware, J. Strand, B. L. T. Plourde, and M. Steffen, *Process Verification of Two-Qubit Quantum Gates by Randomized Benchmarking*, Phys. Rev. A **87**, 030301 (2013).

[51] R. Barends *et al.*, *Superconducting Quantum Circuits at the Surface Code Threshold for Fault Tolerance*, Nature (London) **508**, 500 (2014).

[52] H. Zhu, R. Kueng, M. Grassl, and D. Gross, *The Clifford Group Fails Gracefully to be a Unitary 4-Design*, arXiv:1609.08172.

[53] Y. Nakata and M. Murao, *Diagonal-Unitary 2-Designs and Their Implementations by Quantum Circuits*, Int. J. Quantum. Inform. **11**, 1350062 (2013).

[54] Y. Nakata and M. Murao, *Diagonal Quantum Circuits: Their Computational Power and Applications*, Eur. Phys. J. Plus **129**, 152 (2014).

[55] Y. Nakata, C. Hirche, C. Morgan, and A. Winter, *Decoupling with Random Diagonal Unitaries*, arXiv:1509.05155.

[56] R. A. Low, *Large Deviation Bounds for k-Designs*, Proc. R. Soc. A **465**, 3289 (2009).

[57] A. Kitaev, A. Shen, and M. Vyalyi, *Classical and Quantum Computation* (American Mathematical Society, Boston, 2002).

[58] Y. Nakata, P. S. Turner, and M. Murao, *Phase-Random States: Ensembles of States with Fixed Amplitudes and Uniformly Distributed Phases in a Fixed Basis*, Phys. Rev. A **86**, 012301 (2012).

[59] M. B. Hastings and A. W. Harrow, *Classical and Quantum Tensor Product Expanders*, Quantum Inf. Comput. **9**, 336 (2009).

[60] Y. Nakata, Ph.D. thesis, The University of Tokyo, 2012.

[61] Y. Nakata, M. Koashi, and M. Murao, *Generating a State t-Design by Diagonal Quantum Circuits*, New J. Phys. **16**, 053043 (2014).

[62] R. Ahlswede, H. Aydinian, and L. H. Khachatrian, *Extremal Problems under Dimension Constraints*, Discrete Math. **273**, 9 (2003).

[63] R. Ahlswede, H. Aydinian, and L. H. Khachatrian, *Maximal Antichains under Dimension Constraints*, Discrete Math. **273**, 23 (2003).

[64] A. Roy and A. J. Scott, *Unitary Designs and Codes*, Des. Code Cryptogr. **53**, 13 (2009).

[65] M. Ledoux, *The Concentration of Measure Phenomenon* (American Mathematical Society, Providence, 2001).

[66] J. M. Magán, *Black Holes as Random Particles: Entanglement Dynamics in Infinite Range and Matrix Models*, J. High Energy Phys. 08 (2016) 81.
[67] P. Bocchieri and A. Loinger, *Quantum Recurrence Theorem*, Phys. Rev. **107**, 337 (1957).
[68] M. Serbyn, Z. Papić, and D. A. Abanin, *Local Conservation Laws and the Structure of the Many-Body Localized States*, Phys. Rev. Lett. **111**, 127201 (2013).
[69] D. A. Huse, R. Nandkishore, and V. Oganesyan, *Phenomenology of Fully Many-Body-Localized Systems*, Phys. Rev. B **90**, 174202 (2014).
[70] R. Nandkishore and D. A. Huse, *Many-Body Localization and Thermalization in Quantum Statistical Mechanics*, Annu. Rev. Condens. Matter Phys. **6**, 15 (2015).
[71] S. Sachdev and J. Ye, *Gapless Spin-Fluid Ground State in a Random Quantum Heisenberg Magnet*, Phys. Rev. Lett. **70**, 3339 (1993).
[72] A. Kitaev, http://online.kitp.ucsb.edu/online/entangled15/kitaev/; http://online.kitp.ucsb.edu/online/entangled15/kitaev2/.
[73] A. Kitaev, http://online.kitp.ucsb.edu/online/joint98/kitaev/.
[74] J. Maldacena, S. H. Shenker, and D. Stanford, *A Bound on Chaos*, J. High Energy Phys. 08 (2016) 106.
[75] E. Onorati, O. Buerschaper, M. Kliesch, W. Brown, A. H. Werner, and J. Eisert, *Mixing Properties of Stochastic Quantum Hamiltonians*, arXiv:1606.01914.
[76] D. A. Roberts and B. Yoshida, *Chaos and Complexity by Design*, arXiv:1610.04903.
[77] A. S. Sørensen and K. Mølmer, *Entangling Atoms in Bad Cavities*, Phys. Rev. A **66**, 022314 (2002).
[78] S. Gopalakrishnan, B. L. Lev, and P. M. Goldbart, *Frustration and Glassiness in Spin Models with Cavity-Mediated Interactions*, Phys. Rev. Lett. **107**, 277201 (2011).
[79] P. Strack and S. Sachdev, *Dicke Quantum Spin Glass of Atoms and Photons*, Phys. Rev. Lett. **107**, 277202 (2011).
[80] M. L. Metha, *Random Matrices* (Academic Press, Amsterdam, 1990).
[81] Y. Nakata and T. J. Osborne, *Thermal States of Random Quantum Many-Body Systems*, Phys. Rev. A **90**, 050304(R) (2014).