Catalytic Quantum Randomness

P. Boes,[1] H. Wilming,[1,2] R. Gallego,[1] and J. Eisert[1]
[1]*Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany*
[2]*Institute for Theoretical Physics, ETH Zürich, 8093 Zürich, Switzerland*

(Received 13 June 2018; revised manuscript received 21 August 2018; published 29 October 2018)

Randomness is a defining element of mixing processes in nature and an essential ingredient to many protocols in quantum information. In this work, we investigate how much randomness is required to transform a given quantum state into another one. Specifically, we ask whether there is a gap between the power of a classical source of randomness compared to that of a quantum one. We provide a complete answer to these questions, by identifying provably optimal protocols for both classical and quantum sources of randomness, based on a dephasing construction. We find that in order to implement any noisy transition on a d-dimensional quantum system it is necessary and sufficient to have a quantum source of randomness of dimension $\sqrt{d}$ or a classical one of dimension d. Interestingly, coherences provided by quantum states in a source of randomness offer a quadratic advantage. The process we construct has the additional features to be robust and catalytic; i.e., the source of randomness can be reused. Building upon this formal framework, we illustrate that this dephasing construction can serve as a useful primitive in both equilibration and quantum information theory: We discuss applications describing the smallest measurement device, capturing the smallest equilibrating environment allowed by quantum mechanics, or forming the basis for a cryptographic private quantum channel. We complement the exact analysis with a discussion of approximate protocols based on quantum expanders deriving from discrete Weyl systems. This gives rise to equilibrating environments of remarkably small dimension. Our results highlight the curious feature of randomness that residual correlations and dimension can be traded against each other.

DOI: 10.1103/PhysRevX.8.041016 Subject Areas: Quantum Information

I. INTRODUCTION

Randomness is a central concept and resource in various fields of research in computer science, information theory, and physics, in both the classical and the quantum realm. It is an ingredient to (quantum) algorithm design, a core element in coding and communication protocols, and plays a central role in fundamental aspects of statistical mechanics. In the quantum context, randomness is also increasingly being seen as a valuable resource. A natural question that arises in this context is then how much of it is required to implement a given physical process on a quantum system. Another important question is to what extent the required amount of randomness differs depending on whether an *implicit* or an *explicit* model of randomness is employed. Here, an implicit model of randomness considers the source of randomness (SOR) as a black box that provides coin flips, while an explicit model takes into account the fact that, fundamentally, all systems including the ones provided by the SOR are quantum systems, and hence models the randomness as a quantum state.

In this work, we give a complete answer to both of the above questions. We provide, for both the implicit and explicit model, optimal and tight bounds on the amount of randomness required to implement physical processes on quantum systems. Moreover, we show a strict separation between the above models, in the sense that every physical process can be implemented in the explicit model by using only half the amount of randomness that is required in the implicit model.

Specifically, we use a model of noisy processes—processes that require randomness—known as noisy operations [1]. We study the minimal amount of noise required to implement a large variety of noisy processes and construct protocols that saturate the lower bounds imposed by quantum mechanics. These processes include dephasing and equilibration [2,3], decoherence [4,5], the implementation of measurements [5–7], any transition between two quantum states that requires randomness [1], as well as the novel construction of private quantum channels [8,9].

It is an important aspect of our work that, by virtue of an explicit model, these saturated lower bounds also translate into bounds on the physical size of a SOR. This insight allows us to construct, for particular processes, the smallest decohering

environment or measurement device compatible with quantum mechanics [4]. In other words, it provides an understanding of the smallest equilibrating environment [2] possible. The surprisingly small size that suffices for an environment to be equilibrating challenges the commonly held view that such decohering baths should necessarily feature a large dimension.

A further notable feature of the protocols that we construct is that they are catalytic: The same unit of randomness can be reused for different processes [10]. It is also robust, in the sense that we do not require perfect control in either the states prepared by the SOR or the timing of the process, and further recurrent, in the sense that, for large system dimension d, continuous time versions of our noisy processes maintain a state close to the desired final state for times $\tau \propto \sqrt{d}$, at which point the system recurs to the initial state.

II. CLASSICAL VERSUS QUANTUM NOISE

Let us begin with discussing in more detail the difference between classical and quantum uses of randomness. Consider initial and final (mixed) states ρ, ρ' on a Hilbert space $\mathcal{H}_S$ of dimension $\dim(\mathcal{H}_S) = d$. We are concerned with the possibility of implementing a transition $\mathcal{E}(\rho) = \rho'$, where $\mathcal{E}$ represents a noisy process. There exist different ways of modeling the maps $\mathcal{E}$, which we now explain in detail.

In a classical, implicit model of the SOR one assumes a discrete random variable J that is uniformly distributed over m possible values. Depending on the value of j, one implements a given unitary transformation U_j, which gives rise to the operations

$$\mathcal{E}_C^m(\cdot) = \frac{1}{m}\sum_{i=1}^{m} U_i \cdot U_i^\dagger. \tag{1}$$

If there exist $\mathcal{E}_C^m$ so that a transition is possible, we simply denote it by $\rho \overset{m}{\to}_C \rho'$. In contrast, in an explicit quantum model, the SOR is a quantum system R in the maximally mixed state of dimension m, which we denote by $\mathbb{I}_m := (1/m)\mathbb{1}$, with $\mathbb{1}$ being the identity matrix. In this model, noisy processes are any effect of a unitary joint evolution of the compound,

$$\mathcal{E}_Q^m(\cdot) = \mathrm{tr}_R[U(\cdot \otimes \mathbb{I}_m)U^\dagger]. \tag{2}$$

As in the classical case, we write $\rho \overset{m}{\to}_Q \rho'$ whenever the transition is possible.

The set of transitions that can be implemented with both classical and quantum noise coincides if the amount of noise—quantified by the dimension m—is unbounded. In this case we have

$$\rho \overset{\infty}{\to}_C \rho' \Leftrightarrow \rho \overset{\infty}{\to}_Q \rho' \Leftrightarrow \rho \succ \rho', \tag{3}$$

where we use the symbol "$\succ$" to indicate that ρ majorizes ρ' [11]. The set of transitions $\rho \overset{\infty}{\to}_Q \rho'$ have been extensively studied as noisy operations [1], where the noise is treated as a free resource and the main concern is to study the possible transitions with unbounded m. In contrast, here we are concerned with treating noise as a valuable resource and focus on the following question: What is the minimal amount of noise—quantified by m—that serves to implement any possible transition between pairs of d-dimensional quantum states fulfilling $\rho \succ \rho'$? We denote these minimal values of d for the classical and quantum case by $m_C^*(d)$ and $m_Q^*(d)$, respectively.

At first glance, one might suspect that $m_C^*(d) = m_Q^*(d)$, with quantum noise offering no advantage over its classical counterpart. That intuition comes from the fact that, although one writes a full quantum description in Eq. (2), the state of R, given by $\mathbb{I}_m$, is nevertheless a quasiclassical state. Hence, it seems reasonable that it could be recast as a classical variable, similarly as in Eq. (1). However, treating the noise as a quantum state allows one to access its quantum degrees of freedom, for example, to create entanglement between the S and R. In other words, one could in principle use quantum correlations to make a more efficient use of the noise yielding $m_C^*(d) > m_Q^*(d)$.

One of the main results of this work is to show that there is indeed a gap between the classical and quantum case. We find that $m_C^*(d) = d > \lceil d^{1/2} \rceil = m_Q^*(d)$, and more importantly, we construct protocols that saturate those bounds. In this way, we provide protocols that use the noise optimally for a large variety of tasks. These protocols also have a number of useful properties, such as allowing one to reuse the noise or being robust under different classes of imperfections. In the subsequent section, we present the key lemma to construct such optimal protocols and then turn to discuss applications and properties in Sec. IV.

III. AN OPTIMAL DEPHASING MAP

For any state transition $\rho \to \rho'$ that is possible under either quantum or classical noisy processes, there exists a corresponding map $\mathcal{E}(\rho) = \rho'$ such that

$$\mathcal{E}(\cdot) = \mathcal{U}' \circ \pi_A \circ \mathcal{U}(\cdot). \tag{4}$$

Here, $\mathcal{U}', \mathcal{U}$ are unitary channels that depend on ρ and ρ'. The map π_A is the dephasing map in a fixed orthonormal basis $A = \{|i\rangle\}_{i=1}^d$, defined as

$$\langle i|\pi_A(\rho)|j\rangle = \langle i|\rho|j\rangle \delta_{i,j}, \tag{5}$$

with $\delta_{i,j}$ being the Kronecker delta. This follows from the Schur-Horn theorem [12] together with Eq. (3) and was used to bound the required randomness for noisy processes already in Ref. [13]. Since the unitary channels $\mathcal{U}', \mathcal{U}$ do not require the use of any SOR by definition, we see from

Eq. (4) that noise is required only for the implementation of the dephasing map π_A. In turn, Eq. (4) implies that whether $\mathcal{E}$ represents a quantum noisy process or a classical one depends only on the particular implementation of this dephasing map: Any construction of π_A in the form of Eq. (2) with m-dimensional SOR implies also that $\mathcal{E}$ is a map $\mathcal{E}_Q^m$, while any construction of it in the form of Eq. (1) implies that $\mathcal{E}$ is of the form $\mathcal{E}_C^m$.

Understanding the amount of randomness required to implement the dephasing map therefore is key to understanding the amount of randomness required to implement any noisy process. The following lemma provides a protocol implementing a dephasing map in any basis, using an explicit model model of noise and requiring a SOR of dimension $m = \lceil d^{1/2} \rceil$.

Lemma 1 (Catalytic quantum dephasing).—For any integer d and basis A there exists a unitary U, so that

$$\mathrm{tr}_R[U(\cdot \otimes \mathbb{I}_{\lceil d^{1/2} \rceil})U^\dagger] = \pi_A(\cdot), \tag{6}$$

$$\mathrm{tr}_S[U(\rho \otimes \mathbb{I}_{\lceil d^{1/2} \rceil})U^\dagger] = \mathbb{I}_{\lceil d^{1/2} \rceil} \quad \forall\ \rho. \tag{7}$$

Proof.—Assume first that $\sqrt{d} = m \in \mathbb{N}$. Now, let $\{U_i\}$ be a unitary operator basis for $\mathcal{B}(\mathcal{H}_R)$, that is, a collection of $m^2 = d$ unitary operators $U_i \in \mathcal{B}(\mathcal{H}_R)$, such that

$$\frac{1}{m}\mathrm{tr}(U_i U_j^\dagger) = \delta_{i,j} \tag{8}$$

for all i, j. Such a basis exists for every m [14,15]. We now define the unitary,

$$U = \sum_{i=1}^{d} |i\rangle\langle i| \otimes U_i, \tag{9}$$

where the $\{|i\rangle\}$ are elements of the basis A in which we intend to pinch. Then, for any density matrix ρ on $\mathcal{H}_S$,

$$\mathrm{tr}_R[U(\rho \otimes \mathbb{I}_m)U^\dagger] = \sum_{i,j} |i\rangle\langle i|\rho|j\rangle\langle j| \frac{1}{m}\mathrm{tr}(U_i U_j^\dagger) \tag{10}$$

$$= \sum_{i,j} |i\rangle\langle i|\rho|j\rangle\langle j|\delta_{i,j} = \pi_A(\rho). \tag{11}$$

Lastly, note that Eq. (7) follows simply by

$$\mathrm{tr}_S[U(\rho \otimes \mathbb{I}_m)U^\dagger] = \sum_i \langle i|\rho|i\rangle U_i \mathbb{I}_m U_i^\dagger = \mathbb{I}_m. \tag{12}$$

In the case where $\sqrt{d}$ is not an integer, we can use the same construction with a source of randomness of dimension $m = \lceil d^{1/2} \rceil$ by simply not exhausting all possible m^2 possible unitaries U_i on R. ∎

The protocol of Lemma 1 is optimal, in the sense that it is impossible to implement the dephasing map with $m < \lceil d^{1/2} \rceil$. This can be seen by noting that for any basis A one can always choose an initial pure state ρ so that $\pi_A(\rho) = \mathbb{I}_d$. Using the preservation of the von Neumann entropy under unitaries and the Lieb-Araki triangle inequality, one finds that $m \geq \sqrt{d}$ (see Appendix A). This implementation of the dephasing map compares with the best value known to date of $m = d$, proven in Ref. [13], whose implementation can in fact be shown to correspond to a classical noisy operation of the form Eq. (1), as we see later.

A. Catalyticity

Equation (7) states that the dephasing operation defined in Lemma 1 leaves the state of R invariant, or in other words, that the noise is catalytic [10,16–18]. This property has numerous useful applications. For instance, an immediate corollary of the lemma is that one can locally dephase an arbitrarily large number of uncorrelated systems, each of them of dimension at most d, by using a single noise system R of dimension $\lceil d^{1/2} \rceil$. More formally, we have that for any set of states $\{\rho^i\}_{i=1}^N$ there exists a unitary U so that

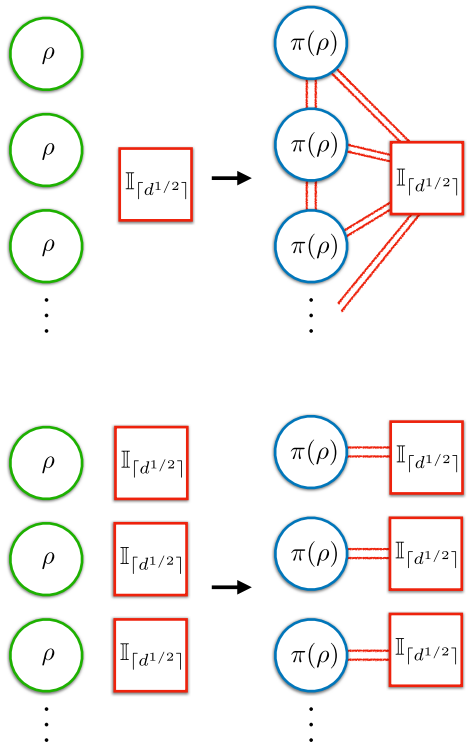


FIG. 1. Two possible ways of dephasing and the resulting correlation structure. Top: A sequence of systems in state ρ is dephased using a single state of randomness, with correlations being established between all systems involved. The local marginals of the resulting global state Eq. (13) are the dephased initial states. Bottom: In order to avoid correlations between the systems, one can instead use additional and unused randomness.

$$\mathrm{tr}_R[U(\rho^i_{S_1}\otimes\cdots\otimes\rho^i_{S_N}\otimes\mathbb{I}_{\lceil d^{1/2}\rceil})U^\dagger]=\rho'_{S_1,\ldots,S_N}, \quad (13)$$

where $\rho'_{S_i}=\pi_{A_i}(\rho^i_{S_i})$. This follows by simply iterating the unitaries of Lemma 1 with all the subsystems and reusing the noise, as illustrated in the top of Fig. 1. In contrast, if the noise would not have the property of being catalytic, then it would be necessary to employ a new mixed state for each of the subsystems, in which case an amount of randomness proportional to N would be required (bottom of Fig. 1). It is important to note, however, that reusing the randomness comes at the cost of correlating the subsystems amongst each other. Hence, if a protocol requires for the individual systems to remain uncorrelated, one still has to resort to a scheme whose required randomness scales linearly with the number of subsystems.

As sketched already, dephasing can be related to many processes that require noise, both in engineered as well as in equilibrating natural quantum processes. In the remainder of this work, we discuss and present applications of Lemma 1 to these processes.

IV. APPLICATIONS

A. Minimal noise for state transitions

As a first application, we prove the tight bounds for noisy operations presented in Sec. II. Formally, given a Hilbert space $\mathcal{H}_S$ with $\dim(\mathcal{H}_S)=d$, we define the minimal noise for the classical and quantum case as

$$m^*_C(d)\coloneqq\arg\min_m \rho\xrightarrow{m}_C\rho' \quad \forall\,\rho,\rho'\in\mathcal{B}(\mathcal{H}_S)|\rho\succ\rho', \quad (14)$$

$$m^*_Q(d)\coloneqq\arg\min_m \rho\xrightarrow{m}_Q\rho' \quad \forall\,\rho,\rho'\in\mathcal{B}(\mathcal{H}_S)|\rho\succ\rho'. \quad (15)$$

In the following lemma we find the values of the above quantities, thus providing the smallest SOR that suffices to perform any transition between two states $\rho\succ\rho'$. Note, however, that it is possible for particular transitions to require even less randomness or none at all.

Lemma 2 (Optimal source of randomness for state transitions).—Any state transition of a d-dimensional system that is possible under noisy processes, in the sense of Eqs. (14) and (15), can be implemented using an amount of classical and quantum noise given by

$$m^*_C(d)=d, \quad (16)$$

$$m^*_Q(d)=\lceil d^{1/2}\rceil. \quad (17)$$

Proof.—Here, we prove only that the above values are sufficient. For the corresponding necessary conditions (and ϵ-approximate versions of the above), see Appendix A. Equation (17) follows from combining Eq. (4) with the dephasing construction in Lemma 1. To see Eq. (16), consider the unitary

$$V=\sum_{i=1}^{d}|i\rangle\langle i|_S\otimes X^i_R, \quad (18)$$

where X is the generalized Pauli matrix defined as

$$X|i\rangle=|(i+1)\bmod d\rangle. \quad (19)$$

As shown in Ref. [13], this unitary implements the dephasing map,

$$\mathrm{tr}_R[V(\rho\otimes\mathbb{I}_d)V^\dagger]=\frac{1}{d}\sum_{i,j}\langle i|\rho|j\rangle|i\rangle\langle j|\mathrm{tr}(X^{i-j})=\pi_A(\rho). \quad (20)$$

V is the local Fourier transform of a unitary leading to a channel of the form Eq. (1): there exists a unitary F and a basis $\{|\tilde{j}\rangle=F^\dagger|j\rangle\}$ such that

$$\tilde{V}\coloneqq(\mathbb{1}\otimes F)V(\mathbb{1}\otimes F^\dagger)=\sum_{j=1}^{d}Z^j\otimes|\tilde{j}\rangle\langle\tilde{j}|. \quad (21)$$

Here,

$$Z=\sum_j\omega_d^j|j\rangle\langle j| \quad (22)$$

is the generalized Pauli matrix conjugate to X and ω_d the dth root of unity. Since the maximally mixed state is unitarily invariant, $\tilde{V}$ implements the dephasing map, and its action on the system S can be represented as

$$\rho\mapsto\mathrm{tr}_R[\tilde{V}(\rho\otimes\mathbb{I}_d)\tilde{V}^\dagger]=\frac{1}{d}\sum_{j=1}^{d}Z^j\rho Z^{-j}. \quad (23)$$

Thus the dephasing map can be implemented with a classical SOR of dimension d. ∎

This lemma proves a conjecture in Ref. [13], where the possibility of strengthening their bound $m^*_Q(d)=d$ to the present one was already raised.

In complete analogy to the discussion in Sec. III A and Fig. 1, we can also use the catalytic properties of the source of randomness to implement state transitions locally from an initially uncorrelated state and using a fixed-size source of randomness. More concretely, let $\{\rho^i\}_{i=1}^N$ and $\{\sigma^i\}_{i=1}^N$ be d-dimensional quantum states such that $\rho^i\succ\sigma^i$ for all $i=1,\ldots,N$. Then there exists a unitary U such that

$$\mathrm{tr}_R[U(\rho^1_{S_1}\otimes\cdots\otimes\rho^N_{S_N}\otimes\mathbb{I}_{\lceil d^{1/2}\rceil})U^\dagger]=\rho'_{S_1,\ldots,S_N}, \quad (24)$$

with $\rho'_{S_i}=\sigma^i$. To see this, we recall from the discussion in Sec. III A that the transition $\rho^i\to\sigma^i$ can be implemented composing unitary channels and dephasing maps. Hence, $\mathcal{E}(\rho^1_{S_1}\otimes\cdots\otimes\rho^1_{S_1})=\sigma^1_{S_1}\otimes\cdots\otimes\sigma^1_{S_1}$, with

$$\mathcal{E} = \bigotimes_{i=1}^{N} \mathcal{U}'_{S_i} \circ \bigotimes_{i=1}^{N} \pi_{A_1} \circ \bigotimes_{i=1}^{N} \mathcal{U}_{S_1}. \tag{25}$$

Now, using Eq. (13) we see that it is possible to dephase locally—that is, perform locally the same transition as the one implemented by the second map on the rhs of Eq. (25)—using a single source of randomness of dimension $\lceil d^{1/2} \rceil$, at the cost of creating correlations between the subsystems. Hence, composing the local unitaries with the local dephasing of Eq. (13), we obtain a map that locally implements the same transition as $\mathcal{E}$, as captured by Eq. (24).

B. Smallest possible decohering environment and measurement device

A further application of our results is to the physical mechanism of decoherence and implementing a measurement in quantum mechanics, which can indeed be seen as a special case of a noisy operation, since it requires randomness. Both applications follow from the fact that a quantum source of randomness can be seen as half of a maximally entangled system.

It is useful to first discuss decoherence. To do so, we make use of the fact that the usual decoherence mechanism is, in a sense, simply a purified version of the system-environment interactions that are toy modeled by noisy operations. Let $|\psi\rangle \in \mathcal{H}_S$ be an initial state vector of a d-dimensional system and $|\phi\rangle$ be the initial state vector of the environment. According to the decoherence mechanism, the unitary joint evolution of system and bath is generated by a Hamiltonian whose interaction term picks out, or einselects, a preferred basis in which it decoheres the system [4]. We are now interested in the smallest possible size of the environment that achieves this. Let us label the system basis that is einselected by $A = \{|i\rangle\}$ and assume that $|\phi\rangle$ is a maximally entangled d-dimensional and bipartite state vector over systems E_1 and E_2. We then define the unitary

$$U = U_{SE_1} \otimes \mathbb{1}_{E_2}, \tag{26}$$

where U_{SE_1} is the unitary defined in Eq. (9) that acts on systems S and E_1. As is clear from the above, this unitary will have the effect that

$$\mathrm{tr}_E[U|\psi\rangle\langle\psi| \otimes |\phi\rangle\langle\phi|U^\dagger] = \pi_A(|\psi\rangle\langle\psi|), \tag{27}$$

meaning that even in this purified picture only an environment of the size of the system is required to produce decoherence.

Let us now turn to the smallest possible measurement device. For simplicity, we consider only projective measurement schemes: Suppose we are given a system in some initial state vector $|\psi\rangle$ and some set of projective measurement operators $\{M_i = |i\rangle\langle i|\}, i \in \{1, \ldots, d\}$. Then a measurement process consists of the following steps. A bipartite measurement device, initially in state vector $|\phi\rangle$, consisting of a d-dimensional pointer system P and a remainder R, whose dimension we are interested in bounding, and a unitary W with the effect that

$$\mathrm{Tr}_R[W|\psi\rangle\langle\psi| \otimes |\phi\rangle\langle\phi|W^\dagger] = \sum_i p_i |i, P_i\rangle\langle i, P_i|, \tag{28}$$

where $p_i = \mathrm{tr}(M_i|\psi\rangle\langle\psi|)$ and $\{|P_i\rangle\}$ form an orthonormal basis for the pointer system. Using the above results, we can easily construct a measurement process as follows. Let the initial state vector of the measurement device be $|\phi\rangle = |0\rangle_P \otimes |\phi^+\rangle_R$, where $|\phi^+\rangle$ is a bipartite, d-dimensional, maximally entangled state vector. Further, let $\{V_i\}$ be unitaries defined by the action

$$V_i|i, 0\rangle = |i, P_i\rangle. \tag{29}$$

Finally, define the unitary

$$W = \sum_i |i\rangle\langle i| \otimes V_i \otimes (U_i)_{R_1} \otimes \mathbb{1}_{R_2}, \tag{30}$$

where the unitaries U_i form an operator basis as before. Then, it is easy to verify that $|\phi\rangle$ and W together satisfy Eq. (28). This shows that in principle one requires a measurement device (including the pointer variable) whose size is only twice that of the system to be measured to implement a projective measurement as a physical process. Using entropic arguments one can again show that this is also the smallest possible measurement device. Note that the register R is exclusively used as a source of randomness in this protocol. Thus, if we are willing to give up the assumption that the initial state of the measurement device is pure, then it suffices to keep only part R_1 in a maximally mixed state. Clearly, these results can also be read as providing the minimal dimension of an environment that equilibrates a quantum system of dimension d [2,3].

C. Universal dephasing machine

In Sec. III, we show that with the aid of a noise system R in state $\mathbb{I}_{\lceil d^{1/2} \rceil}$ it is possible to perform a protocol U which has the effect of implementing the dephasing map π_A on the system S. We now investigate which map is induced on S if the same unitary is applied with a system R in a state σ different from $\mathbb{I}_{\lceil d^{1/2} \rceil}$. We show that U brings the system closer to $\pi_A(\rho)$ for any initial states ρ and σ. Also, we find that iterating the same protocol U with a sufficiently large sequence of imperfect noise states of R brings the system S exponentially close (in the number of iterations) to its dephased state. In this sense, U acts as a universal dephasing machine (Figs. 2 and 3): an iterated use of the same protocol U dephases the state of S for large families of states on R acting as a SOR. Hence, one can

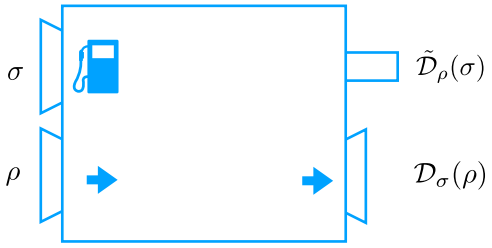


FIG. 2. Single instance of "universal dephasing machine." We interpret the process $\rho \otimes \sigma \to U(\rho \otimes \sigma)U^\dagger$ as a dephasing machine that takes the state σ as fuel and transfers the input state ρ into the output state $\mathcal{D}_\sigma(\rho)$ and "waste" $\tilde{\mathcal{D}}_\rho(\sigma)$.

implement this protocol universally as a "black box," without having to know the actual state of R.

1. Imperfect noise and convergence to the dephased state

Let $\mathcal{D}_\sigma(\cdot)$ denote the map

$$\mathcal{D}_\sigma(\cdot) \coloneqq \mathrm{tr}_R[U(\cdot \otimes \sigma)U^\dagger], \tag{31}$$

where U is the unitary of Lemma 1. In Appendix B, we show that, for any ρ and σ,

$$\mathcal{D}_\sigma(\pi(\rho)) = \pi(\mathcal{D}_\sigma(\rho)) = \pi(\rho), \tag{32}$$

$$\|\mathcal{D}_\sigma(\rho) - \pi(\rho)\|_1 \leq \|\sigma - \mathbb{I}_{\lceil d^{1/2} \rceil}\|_1, \tag{33}$$

where we have dropped the subscript A. These properties imply that, independently of the actual state σ, the system S is brought closer to the dephased state $\pi(\rho)$ while keeping its diagonal invariant. This follows from the data-processing inequality [7]

$$\|\mathcal{D}_\sigma(\rho) - \pi(\rho)\|_1 = \|\mathcal{D}_\sigma(\rho) - \mathcal{D}_\sigma(\pi(\rho))\|_1 \leq \|\rho - \pi(\rho)\|_1.$$

Using those properties, one can show that by repeating the process sequentially (see Fig. 2, top) the system is eventually dephased for large classes of states σ. In fact, one can show that (see again Appendix B)

$$\|\mathcal{D}_\sigma^n(\rho) - \pi(\rho)\|_1 \leq \|\sigma - \mathbb{I}_{\lceil d^{1/2} \rceil}\|_1^n, \tag{34}$$

where $\mathcal{D}_\sigma^n(\rho)$ denotes the repeated application of $\mathcal{D}_\sigma$. This means that, given σ such that $\|\sigma - \mathbb{I}_{\lceil d^{1/2} \rceil}\|_1 < 1$, the dephased state is approached exponentially fast. Note that another corollary of the above properties is that the map $\mathcal{D}_\sigma$ can only increase the von Neumann entropy of its input, which is formally proven in Appendix B 1.

2. Reusing the randomness

In the case of R being in the state $\mathbb{I}_{\lceil d^{1/2} \rceil}$, we show in Sec. III A that it remains unchanged and, thus, the noise is reusable. A natural question is then what happens to the state of R when it is in an arbitrary state σ. Let $\tilde{\mathcal{D}}_\rho$ denote the map

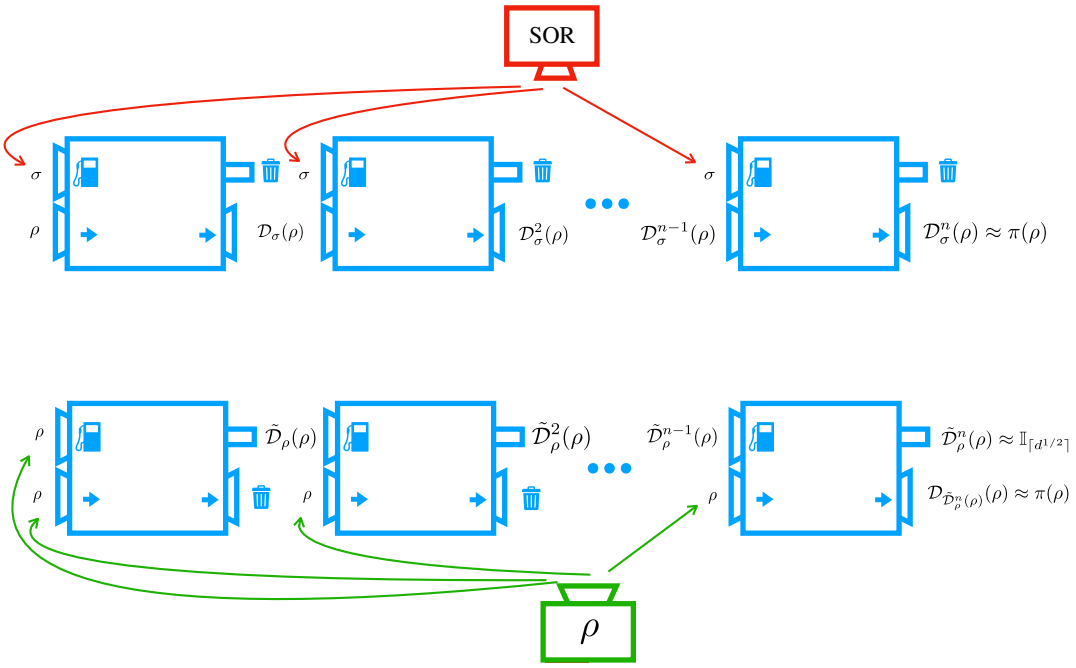


FIG. 3. Top: Repeated application on single input state approximates dephasing map. Bottom: Producing the dephased state when there is no SOR. If $\|\rho - \mathbb{I}_d\|_1 < 1$, then the necessary amount of randomness for dephasing can be distilled by repeated application of the universal dephasing machine.

$$\tilde{\mathcal{D}}_\rho(\cdot) \coloneqq \mathrm{tr}_R[U(\rho \otimes \cdot)U^\dagger]. \tag{35}$$

It follows simply from Eq. (12) that $\tilde{\mathcal{D}}_\rho$ is just a mixture of unitaries, hence bringing R closer to the maximally mixed state. Indeed, following arguments analogous to the ones of Sec. IV C 1 (see Appendix B), one can show that there exist choices for the unitary operator basis of Lemma 1 so that the final state of R fulfills

$$\|\tilde{\mathcal{D}}_\rho(\sigma) - \mathbb{I}_{\lceil d^{1/2}\rceil}\|_1 \leq \|\rho - \mathbb{I}_d\|_1, \tag{36}$$

and analogously it converges as

$$\|\tilde{\mathcal{D}}^n_\rho(\sigma) - \mathbb{I}_{\lceil d^{1/2}\rceil}\|_1 \leq \|\rho - \mathbb{I}_d\|_1^n. \tag{37}$$

Altogether we conclude not only that the noise can be reused, but furthermore, that it improves its quality converging exponentially fast to a state of perfect noise, provided that the initial state ρ is mixed enough to start with (as given by the condition $\|\rho - \mathbb{I}_d\|_1 < 1$). The fact that the noise system is brought closer to the maximally mixed state allows one to implement a distillation protocol such as the one depicted in Fig. 3 (bottom). There, one has a single source providing copies of a given initial state ρ. One aims at dephasing each subsystem locally, similarly to what is done with a perfect noise system in Eq. (13). Here, one can take one copy ρ playing the role of R for some iterations until it is brought close enough to the maximally mixed state, which will happen exponentially quickly, given Eq. (37). Then, using Eq. (34), one can ensure that all the new copies of ρ can be locally dephased.

3. Time control for the dephasing machine and recurrence

Thus far we have left unspecified how the dephasing of the machine would physically be implemented. One concern here may be that the dephasing properties heavily rely on very precise time control of the evolution under the associated Hamiltonian $H = i\log(U)$. However, the numerical simulations depicted in Fig. 4 strongly indicate that, as the system dimension becomes large, H produces an evolution that is close to $\mathcal{D}_\sigma(\cdot)$ for a time span that scales exponentially with the size of S. Indeed, for prime power dimensions and the case $\sigma = \mathbb{I}_{\lceil d^{1/2}\rceil}$, we find analytically that integer iterations of the application of the dephasing unitary always yield the exact dephasing map, up to a recurrence point, at which the original state is returned. See Appendix C for details. The numerical simulations above complement this and suggest that this recurrence property holds not only for integer iterations of the application of the dephasing unitary, but also for intermediate times.

We hence expect that in the limit of very large dimensions, this equilibrating behavior [2,3] becomes arbitrarily good and the state $\rho(t)$ remains close to the equilibrium state $\pi(\rho)$ for a time exponential in the system size. This means that the universal dephasing machine can be made robust in time, in the sense that it does not require exact control over the timing and the dephasing is maintained for long timescales.

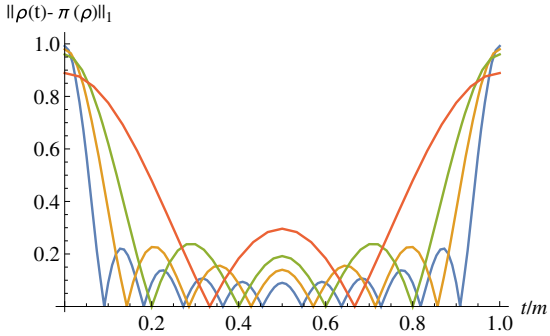


FIG. 4. Numerical simulations of the dephasing map that is induced by the noisy operation Eq. (9) for continuous time and system dimensions $d = m^2 = 9, 25, 49, 121$ (red, green, yellow, blue lines). Shown is the trace-norm distance between the time-evolved state $\rho(t)$ and the pinched state $\pi(\rho)$ as a function of rescaled time t/m. The initial state is a maximally coherent state $(1/\sqrt{d})\sum_i |i\rangle$. The graph shows that, while for integer times (with respect to the bath dimension) the dephasing is always exact, for noninteger times the deviation from exact dephasing becomes small with increasing dimension. The numerically obtained deviation at $t/m = 0.5$ seems compatible with a scaling as $1/m = 1/\sqrt{d}$, but we leave open to derive the exact scaling behavior.

D. Entanglement-assisted private quantum channel

In this section, we apply our results to the construction of a cryptographic protocol known as a private quantum channel (PQC). In a PQC setting, two parties, Alice and Bob, would like to communicate quantum data privately, that is, without an eavesdropper being able to intercept and retrieve the data. To achieve this they share a secret key. We now first briefly explain PQCs using classical secret keys and then provide a construction where the classical key k is substituted for a "quantum key" in the form of a minimal number of entangled bits. In the following, we denote by $\mathcal{S}(\mathcal{H})$ the set of normalized quantum states on the Hilbert space $\mathcal{H}$. Formally, in the classical setting, a (δ, ϵ) PQC is a set of pairs of encoding and decoding completely positive trace-preserving (CPTP) maps $\mathcal{X}_k : \mathcal{S}(\mathcal{H}_A) \to \mathcal{S}(\mathcal{H}_{A'})$ and $\mathcal{Y}_k : \mathcal{S}(\mathcal{H}_{A'}) \to \mathcal{S}(\mathcal{H}_A)$ that can be locally implemented by the sending and receiving parties, respectively, where k denotes the secret key that is shared by Alice and Bob. We think of the key k as a random variable and assume that the key k occurs with probability $p(k)$. These channels then have to fulfill the following conditions [19]. Firstly, there exists a fixed element $\tau \in \mathcal{S}(\mathcal{H}'_A)$, such that

$$\sup_{\rho_{A,B} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)} \left\| \left(\sum\nolimits_k p_k \mathcal{X}_k \otimes \mathrm{id} \right)(\rho_{A,B}) - \tau \otimes \rho_B \right\|_1 \leq \epsilon, \tag{38}$$

where $\rho_{A,B}$ is any extension of the input state ρ_A to a larger Hilbert space and $\rho_B = \mathrm{tr}_A(\rho_{A,B})$. And secondly,

$$\sup_{\rho \in \mathcal{S}(\mathcal{H}_A)} \left\| \sum\nolimits_k p_k \mathcal{Y}_k \circ \mathcal{X}_k(\rho) - \rho \right\|_1 \leq \delta. \tag{39}$$

Equation (38) warrants (approximate) security from eavesdropping, while Eq. (39) warrants the channel's (approximate) reliability. The reason that the security is defined over all possible extensions is that the eavesdropper may initially be entangled with part of the unencrypted message. Finally, a (0,0) PQC is called an *ideal* PQC.

PQCs have been well studied for the case in which Alice and Bob share a classical key [8,9,19–22]. In this case, and if $\mathcal{X}_k$ is unitary, the encoding corresponds to a classical noisy process and a key of length at least $[2 - O(\epsilon)]n$ is necessary for the ϵ-secure transmission of n qubits [8,9,19,23].

Here, in contrast, we consider a setting in which Alice and Bob share a quantum key in the form of entangled quantum states. We use our dephasing map to construct an ideal private quantum channel that requires n shared ebits of entanglement to transmit n qubits of quantum data. As with the dephasing map, this value can again be shown to be optimal, in the sense that no implementation of an ideal PQC as a noisy operation can require fewer ebits (a result that extends to approximately ideal PQCs). It improves on the only other discussion of PQCs that uses entanglement known to the authors, in Ref. [25]. There, an ideal PQC is constructed that applies techniques from classical PQCs and hence achieves only "classical" efficiency by requiring $2n$ ebits for n transmitted qubits.

The idea behind our construction is straightforward (see Fig. 5). Given an n-qubit system S, let U_I and U_J denote the dephasing unitaries Eq. (9) whose projective part corresponds to the two orthonormal bases $I = \{|i\rangle\}_{i=1}^d$ and $J = \{|j\rangle\}_{j=1}^d$ for $\mathcal{H}_S$. If Alice and Bob share n ebits, and assuming for convenience that n is even, Alice can split the ebits into two halves, which we call E_1 and E_2. She then applies U_I to S and her local share of E_1, followed by applying U_J to S and her half of E_2. It is easy to check that if I and J are mutually unbiased, that is, if

$$|\langle i|j\rangle|^2 = \frac{1}{d}, \quad \forall\ i, j, \tag{40}$$

then this results in the completely depolarizing channel. That is, the map

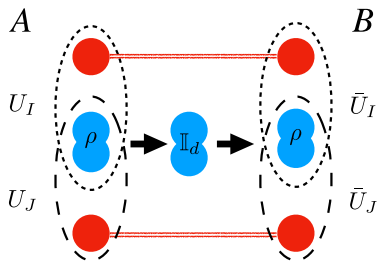


FIG. 5. Illustration of our quantum PQC for the case $n = 2$. To encode a 2-qubit state ρ (blue), Alice applies the dephasing unitaries U_I and U_J to the system and one half of an ebit (red) each, where I and J can be any mutually unbiased bases. This maps ρ into the maximally mixed state exactly, so that an eavesdropper cannot learn anything about ρ even if she was initially entangled with part of it. Bob, in order to decode, applies the conjugate of the two above unitaries and thereby retrieves the state exactly.

$$\mathcal{X}(\cdot) \coloneqq \mathrm{tr}_E[U_J U_I(\cdot \otimes |\phi^+\rangle\langle\phi^+|_{E_1} \otimes |\phi^+\rangle\langle\phi^+|_{E_2}) U_I^\dagger U_J^\dagger], \tag{41}$$

where $|\phi^+\rangle$ represents an $n/2$-ebit state vector, has the property that

$$\mathcal{X}(\rho) = \mathbb{I}_d, \quad \forall \rho \in \mathcal{D}(\mathcal{H}_S). \tag{42}$$

This ensures perfect secrecy, since the completely depolarizing channel necessarily also removes all correlations to other systems [20]. Upon receipt of S, Bob can then apply the complex conjugate of the encoding unitaries to his share of the ebits to retrieve the original state. See Appendix D for the formal proofs.

This construction has a number of interesting features, some of which, however, are already present in the construction of Ref. [25]. For instance, it is catalytic in the sense that, at the end of the transmission process, in case no eavesdropper has interacted with the sent data, all of the entanglement is returned in its initial state and can be reused for future rounds of transmission. Moreover, the scheme allows for error correction, efficient authentication, and recycling of some of the entanglement in case eavesdropping has occurred. We refer the reader to Appendix D for a discussion of these properties.

V. DEPHASING WITH QUANTUM EXPANDERS

The protocol presented in Lemma 1 allows one to dephase perfectly a d-dimensional system given a SOR of dimension of $m = \lceil d^{1/2} \rceil$. This very same protocol, when applied to an imperfect SOR of dimension m but not in the maximally mixed state, yields, as shown in Sec. IV C 1, a convergence to the dephased state when the protocol is iterated. In this section, we study a complementary protocol that provides astonishingly fast convergence when we have states of the SOR that are maximally

mixed, but of dimension significantly smaller than m. We find a protocol that yields an exponential convergence to the dephased state with the dimension of the SOR, measured in the 2-norm. This is remarkable, in that it shows that one can obtain an equilibration in 2-norm exponentially quickly in the ancillary dimension. This insight may be seen as being at odds with the intuition that an equilibrating environment should naturally have a large physical dimension. Our approach is based on a machinery of quantum expanders [26–28]. The key insight is that one can trade residual correlations still present in the system with the dimension required for the mixing environment. This feature demonstrates an intriguing feature of randomness.

Theorem 3 (Dephasing with quantum expanders).—For any d-dimensional state ρ, $d = e^2$ with d odd, and an integer k, there exists an $8k$-dimensional quantum system R and a unitary $U \in (8dk)$, such that

$$\|\mathrm{tr}_R[U(\rho \otimes \mathbb{I}_{8k})U^\dagger] - \pi(\rho)\|_2 \leq \sqrt{2d^3}\left(\frac{5\sqrt{2}}{8}\right)^k. \quad (43)$$

The restriction to the dimension is done for pure conceptual simplicity. The argument for the proof, presented in Appendix E, follows from a construction of a classical random walk that acts on the vertices of an expander graph, a Margulis expander [29]. In the present construction, the vertices of the Margulis expander are seen as lines labeled by $q = 1, \ldots, d$ in a $(d \times d)$-dimensional quantum phase space of the d-dimensional quantum system. The central insight is that classical random walks on such lattices are reflected by random walks on Wigner functions defined on $(d \times d)$-dimensional phase spaces, which in turn give rise to random unitary channels on quantum states in d dimensions. The construction laid out in detail in the Appendix E builds upon and draws inspiration from the scheme of Ref. [27], but is in several important ways a new scheme, in particular, in that each line in phase space is treated separately. In this way, the strong mixing properties of the random walk of the Margulis expander graph are not used to show rapid mixing to a maximally mixed state, but in fact to a quantum state with vanishing off-diagonal elements.

VI. SUMMARY AND CONCLUSIONS

We study the problem of implementing state transitions under noisy processes, that is, processes that require randomness. We solve this problem completely by providing optimal protocols for both the case of an implicit, classical model of randomness as well as an explicit, quantum model of randomness. The main building block behind these protocols is the construction of a protocol that performs a dephasing map on an arbitrary quantum state using a SOR of the smallest possible dimension, for both the quantum and classical case. We find that a quantum SOR is quadratically more efficient than its classical counterpart due to quantum correlations, and hence show that an explicit model is strictly more powerful for any dimension $d > 2$.

Once the optimal protocols for dephasing were established, we studied applications such as state transitions in noisy operations, decoherence, and quantum measurements, providing optimal protocols for all of them. An interesting feature of our protocol is that the SOR is not altered during the protocol, meaning that it can be reused to implement further iterations of the above tasks.

We also extend our discussion to the case of imperfect noise and use our results to construct a universal dephasing machine that exhibits robustness both with respect to the noise that fuels it, as well as with respect to the control over timing when running it. Moreover, we use our dephasing as a primitive to construct a novel, ideal private quantum channel. Finally, by putting it into the context of expander graphs, we have seen how such an approximate dephasing is possible with an economical use of noise: Converging in 2-norm to the dephased state with an exponential scaling on the SOR's dimension.

Besides the foundational interest of our construction, which makes precise the way in which the relationship between correlations and randomness in quantum mechanics differs from that in classical mechanics, we expect our dephasing protocol to improve bounds in noisy processes that we have not discussed here, to the extent that introduce a new primitive to constructions in quantum information. Given the pivotal status of randomness in protocols of quantum information processing and in notions of quantum thermodynamics, these results promise a significant number of further practical applications.

ACKNOWLEDGMENTS

P. B. thanks Lluis Masanes, Markus Müller, Jon Richens, and Ingo Roth for interesting conversations, and especially Jonathan Oppenheim for suggesting cryptographic applications of the results. We acknowledge funding from the ERC (TAQ), the DFG (EI 519/14-1, CRC183, FOR 2724), the Templeton Foundation, and the Studienstiftung des Deutschen Volkes. This work has also received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No. 817482 (PASQUANS).

APPENDIX A: LOWER BOUNDS ON DIMENSION OF SOURCE OF RANDOMNESS

In this appendix, we prove the lower bounds in Lemma 2. In fact, we prove them in an approximate setting to show that they are robust to small deviations from exact dephasing. To do so, we call a map $\mathcal{E}_X^m$ ϵ dephasing if, for all operators $\rho \in \mathcal{B}(\mathcal{H}_S)$ and some fixed basis A,

$$\|\mathcal{E}_X^m(\rho) - \pi_A(\rho)\|_1 \leq \epsilon, \quad (A1)$$

where $X \in \{C, Q\}$. Let $m_X^*(d,\epsilon)$ be the smallest value of m such that an ϵ-dephasing map can be realized as a map of the form Eq. (1) for $X = C$ and Eq. (2) for $X = Q$, respectively, $\dim(\mathcal{H}_S) = d$.

We begin with the classical bound. Consider the state vector

$$|A\rangle := \frac{1}{\sqrt{d}} \sum_i |i\rangle. \tag{A2}$$

If it is dephased in the basis $A = \{|i\rangle\}$, it is mapped to the maximally mixed state. We are concerned with deriving the minimal value of m such that $\mathcal{E}_C^m(|A\rangle\langle A|) = \mathbb{I}_d$. For this, note that

$$\mathcal{E}_C^m(|A\rangle\langle A|) = \frac{1}{m} \sum_{j=1}^{m} U_j |A\rangle\langle A| U_j^\dagger. \tag{A3}$$

Clearly, this state has at most rank m, since its support is spanned by m vectors. Moreover, it is easy to see that for any ϵ-dephasing classical map $\mathcal{E}_C^m$,

$$\text{rank } \mathcal{E}_C^m(|A\rangle\langle A|) \geq d\left(1 - \frac{\epsilon}{2}\right), \tag{A4}$$

which implies

$$m_C^*(d,\epsilon) \geq m \geq \max\left\{2, d\left(1 - \frac{\epsilon}{2}\right)\right\}, \tag{A5}$$

where we also use that any nontrivial source of randomness must be at least two dimensional.

To see Eq. (A4), consider any state ρ of rank k. Then,

$$\|\rho - \mathbb{I}_d\|_1 \geq \|\mathbb{I}_{k,d} - \mathbb{I}_d\|_1 = 2\left(1 - \frac{k}{d}\right), \tag{A6}$$

where $\mathbb{I}_{k,d}$ is a d-dimensional state that is maximally mixed on a subspace of dimension k (and hence has rank k). Using Eq. (A1) and rearranging then gives bound Eq. (A4).

Let us now turn to the quantum case, where we find

$$m_Q^*(d,\epsilon) \geq \max\{2, d^{(1-\epsilon)/2}\epsilon^{\epsilon/2}\}, \quad \forall\ \epsilon \leq \frac{1}{6e}. \tag{A7}$$

First, note that for $d \leq 4$, our optimal construction already yields $m = 2 = \lceil d^{1/2} \rceil$ and that any nontrivial source of randomness must have $m \geq 2$. In the following, we hence assume $d \geq 5$. Now consider again the initial state $|A\rangle\langle A|$. Then, for any ϵ-dephasing map $\mathcal{E}_Q^m$, applying Fannes's inequality yields

$$S[\mathcal{E}_Q^m(|A\rangle\langle A|)] \geq \log d + \epsilon \log\left(\frac{\epsilon}{d}\right). \tag{A8}$$

In the following, let ρ_R' denote the state on the m-dimensional source of randomness after the dephasing map has been applied. From our construction of the exact dephasing map, we know that $m^*(d,\epsilon) \leq \lceil d^{1/2} \rceil$. Hence, in the following we assume $2 \leq m \leq \lceil d^{1/2} \rceil$. Since $\epsilon \leq 1/6e$ and

$$\log(\lceil d^{1/2} \rceil) - \log(d^{1/2}) \leq 1/2, \quad \forall\ d \geq 5, \tag{A9}$$

it follows using Eq. (A8) that

$$S[\mathcal{E}_Q^m(|A\rangle\langle A|)] > \log(\lceil d^{1/2} \rceil) \geq S(\rho_R'). \tag{A10}$$

We finally use the Lieb-Araki triangle inequality, which states that

$$S(\rho_{A,B}) \geq |S(\rho_A) - S(\rho_B)|, \tag{A11}$$

for any bipartite state $\rho_{A,B}$. We can now use this to bound

$$\log m = S(|A\rangle\langle A|) + S(\mathbb{I}_m) = S(U|A\rangle\langle A| \otimes \mathbb{I}_m U^\dagger) \tag{A12}$$

$$\geq |S[\mathcal{E}_Q^m(|A\rangle\langle A|)] - S(\rho_R')| \tag{A13}$$

$$= S[\mathcal{E}_Q^m(|A\rangle\langle A|)] - S(\rho_R') \tag{A14}$$

$$\geq \log(d) + \epsilon \log(\epsilon/d) - \log m. \tag{A15}$$

Hence, we obtain

$$m \geq d^{(1-\epsilon)/2}\epsilon^{\epsilon/2}, \tag{A16}$$

which finishes the proof.

APPENDIX B: UNIVERSAL DEPHASING MACHINE

In this appendix, we provide further details on the results regarding the universal dephasing machine. For convenience, we drop the subscripts for the dephasing maps and the maximally mixed states.

1. Robustness with respect to imperfect noise

Let us first show the following lemma.

Lemma 4 (General properties of $\mathcal{D}_\sigma$).—The family of channels $\mathcal{D}_\sigma$ has the following properties.

(1) Fixed points. All diagonal states are fixed points:

$$\mathcal{D}_\sigma(\pi(\rho)) = \pi(\rho), \quad \forall\ \sigma, \rho. \tag{B1}$$

(2) Invariant diagonal. The channels do not modify the diagonal of any state in the given basis:

$$\pi(\mathcal{D}_\sigma(\rho)) = \pi(\rho), \quad \forall\ \sigma, \rho. \tag{B2}$$

(3) Continuity. The following continuity property holds:

$$\|\mathcal{D}_\sigma(\rho)-\pi(\rho)\|_1 \le \|\sigma-\mathbb{I}\|_1. \tag{B3}$$

Proof.—The first two properties follow from the definition of $\mathcal{D}_\sigma$ in Eq. (31), since

$$\langle k|\mathrm{tr}_B[U(\rho\otimes\sigma)U^\dagger]|k\rangle = \sum_{i,j}\langle k|i\rangle\langle i|\rho|j\rangle\langle j|k\rangle \mathrm{tr}(U_i\sigma U_j^\dagger) \tag{B4}$$

$$= \rho_{k,k}\mathrm{tr}(U_k^\dagger U_k\sigma) = \rho_{k,k}. \tag{B5}$$

The continuity property can be seen as

$$\begin{aligned}\|\mathcal{D}_\sigma(\rho)-\pi(\rho)\|_1 &= \|\mathrm{tr}_B[U(\rho\otimes\sigma)U^\dagger]-\mathrm{tr}_B[U(\rho\otimes\mathbb{I})U^\dagger]\|_1\\ &\le \|U(\rho\otimes(\sigma-\mathbb{I}))U^\dagger\|_1\\ &= \|\rho\otimes(\sigma-\mathbb{I})\|_1\\ &= \|\sigma-\mathbb{I}\|_1,\end{aligned} \tag{B6}$$

where we have used the data-processing inequality and the unitary invariance of the norm. ∎

In particular, the fixed-point property has the following corollaries.

Corollary 5 (Contraction to dephased state).—Let $f(\rho,\rho')$ be any measure of distance between quantum states that fulfills the data-processing inequality, for example, any Renyi divergence or the trace distance [7]. Then,

$$f(\rho,\pi(\rho)) \ge f(\mathcal{D}_\sigma(\rho),\pi(\rho)), \quad \forall\ \sigma. \tag{B7}$$

Choosing $f(\rho,\sigma)$ as the quantum relative entropy $S(\rho\|\sigma)$ and using that $S(\rho\|\pi(\rho)) = S(\pi(\rho)) - S(\rho)$, we then obtain the following corollary.

Corollary 6 (Increasing entropy).—The channels $\mathcal{D}_\sigma$ can only increase the von Neumann entropy:

$$S(\rho) \le S(\mathcal{D}_\sigma(\rho)), \quad \forall\ \sigma. \tag{B8}$$

So far we have considered only single applications of the dephasing map. Let us now consider repeated applications. We thus want to investigate what happens if we have a stream of sources of randomness σ_i and sequentially use them to dephase the system. To this end, we can prove the following lemma.

Lemma 7 (Iterated dephasing).—Let $\{\sigma_i\}_{i=1}^n$ be arbitrary quantum states of dimension $\lceil d^{1/2}\rceil$. Then we have

$$\|(\mathcal{D}_{\sigma_n}\circ\cdots\circ\mathcal{D}_{\sigma_1})(\rho)-\pi(\rho)\|_1 \le \Pi_{i=1}^n\|\sigma_i-\mathbb{I}\|_1. \tag{B9}$$

Proof.—We prove the case $n=2$. The general result follows by iteration. First we use $\pi(\rho)=\pi\circ\mathcal{D}_\sigma(\rho) = \mathcal{D}_\sigma\circ\pi(\rho)$ to write

$$\|(\mathcal{D}_{\sigma_2}\circ\mathcal{D}_{\sigma_1})(\rho)-\pi(\rho)\|_1 = \|(\mathcal{D}_{\sigma_2}-\pi)\circ(\mathcal{D}_{\sigma_1}-\pi)(\rho)\|_1.$$

We can then estimate this norm as

$$\|(\mathcal{D}_{\sigma_2}\circ\mathcal{D}_{\sigma_1})(\rho)-\pi(\rho)\|_1 \le \|\mathcal{D}_{\sigma_1}-\pi\|_{1\to1}\|\mathcal{D}_{\sigma_2}-\pi\|_{1\to1}, \tag{B10}$$

where $\|\cdot\|_{1\to1}$ is the norm on superoperators induced by the 1-norm. From Lemma 4, we can estimate it as

$$\|\mathcal{D}_\sigma-\pi\|_{1\to1} = \max_\rho\|\mathcal{D}_\sigma(\rho)-\pi(\rho)\|_1 \le \|\sigma-\mathbb{I}\|_1. \tag{B11}$$

This step completes the proof. ∎

We thus find that ρ converges exponentially quickly to the dephased state upon iterated application of $\mathcal{D}_\sigma$ provided that $\|\sigma_i-\mathbb{I}\|_1 \le k < 1$ for some k and all σ_i.

2. Action on source of randomness

Let us now consider the action of the dephasing unitary on the source of randomness. Given some ρ, we are thus interested in the channel

$$\tilde{\mathcal{D}}_\rho(\sigma) = \mathrm{tr}_S[U(\rho\otimes\sigma)U^\dagger]. \tag{B12}$$

This channel is always unital; i.e., it fulfills $\tilde{\mathcal{D}}_\rho(\mathbb{I})=\mathbb{I}$ for any ρ. Thus,

$$\|\tilde{\mathcal{D}}_\rho(\sigma)-\mathbb{I}\|_1 \le \|\sigma-\mathbb{I}\|_1. \tag{B13}$$

Let us denote by $\mathcal{R}$ the channel that maps any state into the maximally mixed state, $\mathcal{R}(\sigma)=\mathbb{I}$. Then we have $\mathcal{R}=\tilde{\mathcal{D}}_\rho\circ\mathcal{R}=\mathcal{R}\circ\tilde{\mathcal{D}}_\rho$. By the same arguments as in the previous section, we then obtain the following lemma.

Lemma 8 (Iterated mixing).—Let $\{\rho_i\}_{i=1}^n$ be arbitrary quantum states of dimension d. Then we have

$$\|(\tilde{\mathcal{D}}_{\rho_n}\circ\cdots\circ\tilde{\mathcal{D}}_{\rho_1})(\sigma)-\mathbb{I}\|_1 \le \Pi_{i=1}^n\|\rho_i-\mathbb{I}\|_1. \tag{B14}$$

APPENDIX C: RECURRENCE AND ROBUSTNESS IN TIME

In this appendix, we show that one can choose the operator basis $\{U_i\}$ from Lemma 1 in such a way that the dephasing map exhibits recurrence properties. By recurrence we here mean that applying the dephasing unitary a certain number of times undoes the dephasing, while it keeps it dephased for intermediate times.

To this end, note that one particular realization of this operator basis is the following: Define the unitaries

$$U_{r,s} \coloneqq \tau^{rs}X^rZ^s, \tag{C1}$$

where X, Z are the generalized Pauli matrices defined in Eq. (19) and (22), respectively, and $\tau=-e^{\pi i/m}=-\sqrt{\omega}$.

In the following, expressions are to be taken modulo m, unless specified otherwise. The conjugation relation $XZ = \omega^{-1}ZX$ then gives rise to the following properties in any dimension [30]:

$$U_{r,s}U_{u,v} = \omega^{us-vr}U_{u,v}U_{r,s} = \tau^{us-vr}U_{r+u,s+v}, \tag{C2}$$

$$U_{r,s}^{k} = U_{kr,ks}, \tag{C3}$$

$$U_{r,s}^{\dagger} = U_{-r,-s}, \tag{C4}$$

$$\mathrm{tr}(U_{r,s}) = m\delta_{r,0}\delta_{s,0}. \tag{C5}$$

These imply, in particular, that $\{U_{r,s}\}, r, s \in \{0,\ldots,m-1\}$ form a unitary operator basis of $\mathcal{B}(\mathcal{H})$. Now, while it is clear that $X^m = Z^m = \mathbb{I}$, we can ask for the smallest k such that $U_{r,s}^k = \mathbb{I}$ for all r, s. The above conjugation relations imply that if m is odd, then this value is given by m, while for even m, the answer is $2m$. For instance, in the case of $m = 2$, we have $X^2 = Z^2 = \mathbb{I}$, while $(XZ)^2 = -\mathbb{I}$. Moreover, we can ask for the dependence of the order of the unitaries U_i, by which we here mean the smallest k such that $U_i^k = \mathbb{I}$, i.e., the order of the corresponding element in the Weyl-Heisenberg group, on m. Here, one has that the order of all nontrivial U_i is d, if and only if d is an odd prime. This special property for odd primes will be of key importance to establish recurrence relations in the following. Define the map

$$\pi_m^k(\cdot) = \begin{cases} \mathrm{id}(\cdot) & \text{if } k \bmod m = 0 \\ \pi_A(\cdot) & \text{otherwise,} \end{cases} \tag{C6}$$

where A denotes the orthonormal basis in which the pinching acts, as in the main text. We then have the following lemma.

Lemma 9 (Recurrence for odd prime dimension).—Let $\dim\mathcal{H}_S = m^2$, $\dim\mathcal{H}_R = m$, where m is an odd prime. There exists a unitary V acting on $\mathcal{H}_S \otimes \mathcal{H}_R$ such that

$$\mathrm{tr}_B[V^k(\rho \otimes \mathbb{I}_m)(V^\dagger)^k] = \pi_m^k(\rho). \tag{C7}$$

Proof.—Let $A = \{|r,s\rangle\}_{r,s=1}^m$ be the orthonormal basis of $\mathcal{H}_S$ in which we want to pinch the state ρ. Define

$$V = \sum_{r,s} |r,s\rangle\langle r,s|_S \otimes (U_{r,s})_R, \tag{C8}$$

where the basis with respect to which the operators Eq. (C1) are defined can be chosen arbitrarily. Then, from the properties of these operators, we have

$$\mathrm{tr}_R[V^k(\rho \otimes \mathbb{I}/d)(V^\dagger)^k]$$

$$= \sum_{r,s,u,v} |r,s\rangle\langle r,s|\rho|u,v\rangle\langle u,v| \frac{1}{m}\mathrm{tr}(U_{kr,ks}U_{-ku,-kv}) \tag{C9}$$

$$= \sum_{r,s,u,v} |r,s\rangle\langle r,s|\rho|u,v\rangle\langle u,v| \frac{1}{m}\tau^{k^2(us-rv)}\mathrm{tr}(U_{r-u,s-v}^k) \tag{C10}$$

$$= \sum_{r,s,u,v} |r,s\rangle\langle r,s|\rho|u,v\rangle\langle u,v|\theta_m(k,r,u,s,v) \tag{C11}$$

$$= \pi_m^k(\rho), \tag{C12}$$

where the last line follows because

$$\theta_m(k,r,u,s,v) := \frac{1}{m}\tau^{k^2(us-rv)}\mathrm{tr}(U_{r-u,s-v}^k) = \begin{cases} 1 & \text{if } k \bmod m = 0 \text{ or both } r = u \text{ and } s = v \\ 0 & \text{otherwise.} \end{cases} \tag{C13}$$

■

The reason that this proof works only for odd prime dimensions is that, if m is not prime, then there will exist a k and a, b, c, e such that the lhs of Eq. (C13) is 1 for conditions other than those of Eq. (C13). Furthermore, when $m = 2$, then there will be diagonal elements such that Eq. (C13) is -1 for $k = 2$, and only for $k = 4$ do we get actual recurrence (implying in turn that for $m = 2$ the map is neither the dephasing map nor the identity map).

However, in the following lemma, we show that for any odd dimension we can construct a unitary operator basis that does exhibit recurrence.

Lemma 10 (Recurrence for odd dimension).—Let $\dim\mathcal{H}_S = m^2$, $\dim\mathcal{H}_R = m$, where m is odd. There exists a unitary V acting on $\mathcal{H}_S \otimes \mathcal{H}_R$ such that

$$\mathrm{tr}_B[V^k(\rho \otimes \mathbb{I}_m)(V^\dagger)^k] = \pi_m^k(\rho). \tag{C14}$$

Proof.—Consider the prime factor decomposition of $m = p_1 \ldots p_l$. We can split the Hilbert spaces as

$$\mathcal{H}_R \simeq \bigotimes_{j=1}^{l} \mathcal{H}_j, \tag{C15}$$

where $\dim(\mathcal{H}_j) = p_j$. Moreover, let $A = \{|\mathbf{r},\mathbf{s}\rangle\}$ be an orthonormal basis of $\mathcal{H}_S$, where $\mathbf{r},\mathbf{s} \in \mathcal{S} := \times_{j=1}^{l}\{1,\ldots,p_j\}$, so that $|\mathcal{S}| = m$. Now, we define the unitary

$$V = \sum_{\mathbf{r},\mathbf{s}\in\mathcal{S}} |\mathbf{r},\mathbf{s}\rangle\langle\mathbf{r},\mathbf{s}|_S \otimes \Big(\bigotimes_j U_{r_j,s_j}^{(j)}\Big)_R, \tag{C16}$$

where $U^{(j)}_{r,s}$ acts nontrivially only on $\mathcal{H}_j$ and r_j, s_j denote the jth component of the respective strings. The result now follows in just the same way as in the previous proof, as

$$\mathrm{tr}_B[V^k(\rho\otimes\mathbb{I}/m)(V^\dagger)^k] = \sum_{\mathbf{r},\mathbf{s},\mathbf{u},\mathbf{v}} |\mathbf{r},\mathbf{s}\rangle\langle\mathbf{r},\mathbf{s}|\rho|\mathbf{u},\mathbf{v}\rangle\langle\mathbf{u},\mathbf{v}| \prod_j^l \left(\frac{1}{p_j}\mathrm{tr}(U^{(j)}_{kr_j,ks_j}U^{(j)}_{-ku_j,-kv_j})\right) \tag{C17}$$

$$= \sum_{\mathbf{r},\mathbf{s},\mathbf{u},\mathbf{v}} |\mathbf{r},\mathbf{s}\rangle\langle\mathbf{r},\mathbf{s}|\rho|\mathbf{u},\mathbf{v}\rangle\langle\mathbf{u},\mathbf{v}| \prod_j^l \theta_{p_j}(k,r_j,s_j,u_j,v_j) \tag{C18}$$

$$= \pi^k_m(\rho), \tag{C19}$$

since $k=m$ is by construction the smallest integer such that $k \bmod p_j = 0$ for all j. ∎

Also, it should be noted that the case of even dimension can also be considered very close to a perfect dephasing map: Within the cycle $k\in\{1,\ldots,2m\}$, the only two times at which the above map does not dephase perfectly is at $k=m$ and $k=2m$. At the latter, it yields the identity map, while at the former, it yields the identity map up to sign flips on a subset of its elements.

APPENDIX D: ENTANGLEMENT-ASSISTED PRIVATE QUANTUM CHANNEL

Here, we present the proofs for the ideal PQC presented in the main text and discuss its properties. As our construction does not fit into the usual formal framework of PQCs with classical keys, let us first specify in more detail what we mean by a private quantum channel with a quantum key. We assume that Alice and Bob hold a shared quantum system $K=K_AK_B$ in a state vector $|\Psi\rangle_K$, which we refer to as the key, and that Alice wants to encode a quantum system S with Hilbert space $\mathcal{H}_S$. For notational simplicity, we write $\mathcal{H}_{K_A}=\mathcal{H}_A$ and $\mathcal{H}_{K_B}=\mathcal{H}_B$. Then an ideal private quantum channel with key $|\Psi\rangle_K$ is given by a pair of quantum channels $\mathcal{X}:\mathcal{S}(\mathcal{H}_S\otimes\mathcal{H}_A)\to\mathcal{S}(\mathcal{H}'_S\otimes\mathcal{H}_A)$ and $\mathcal{Y}:\mathcal{S}(\mathcal{H}'_S\otimes\mathcal{H}_B)\to\mathcal{S}(\mathcal{H}_S\otimes\mathcal{H}_B)$ with the following properties. First, there exists a fixed state τ, such that for all auxiliary systems E and all states ρ_{SE} on S and E, we have

$$\mathrm{tr}_K\circ(\mathcal{X}\otimes\mathrm{id}_{K_BE})(\rho_{SE}\otimes|\Psi\rangle\langle\Psi|_K)=\tau\otimes\rho_E. \tag{D1}$$

This implies that an eavesdropper cannot learn anything from the encoded message, even when previously entangled with S. Second, the transmission is reliable; that is, for all states ρ on S, we have

$$\mathrm{tr}_K\circ(\mathcal{Y}\otimes\mathrm{id}_{K_A})\circ(\mathcal{X}\otimes\mathrm{id}_{K_B})(\rho\otimes|\Psi\rangle\langle\Psi|_K)=\rho. \tag{D2}$$

In the following, we show that the construction sketched in the main text fulfills this definition and explore some of its additional properties. We begin with the following lemma.

Lemma 11 (Properties of a private quantum channel).—Let $\rho\in\mathcal{S}(\mathcal{H}_S)$ with $\dim(\mathcal{H}_S)=d$ and let $|\phi^+\rangle\in\mathcal{H}_K=\mathcal{H}_A\otimes\mathcal{H}_B$ be an e-dimensional, maximally entangled bipartite state vector with $e=(\lceil d^{1/2}\rceil)^2$. Then there exist unitaries $U\in\mathcal{B}(\mathcal{H}_S\otimes\mathcal{H}_A), V\in\mathcal{B}(\mathcal{H}_S\otimes\mathcal{H}_B)$ such that

$$\mathrm{tr}_{A,B}[U(\rho\otimes|\phi^+\rangle\langle\phi^+|)U^\dagger]=\mathbb{I}_d,\quad\forall\ \rho, \tag{D3}$$

and

$$VU(\rho\otimes|\phi^+\rangle\langle\phi^+|)U^\dagger V^\dagger=\rho\otimes|\phi^+\rangle\langle\phi^+|,\quad\forall\ \rho. \tag{D4}$$

Proof.—Consider first the case that d is a square number, in which case $e=d$. We can assume without loss of generality that

$$|\phi^+\rangle=|\phi_1^+\rangle\otimes|\phi_2^+\rangle, \tag{D5}$$

where $|\phi_i^+\rangle$ are both $\sqrt{e}$-dimensional maximally entangled state vectors acting on $\mathcal{H}_{A_i}\otimes\mathcal{H}_{B_i}$, respectively, of the form

$$|\phi_i^+\rangle=\frac{1}{e^{1/4}}\sum_{j=1}^{\sqrt{e}}|j,j\rangle_{A_iB_i}. \tag{D6}$$

We can do this because Alice and Bob can always rotate between all maximally entangled states by applying local unitaries and hence prepare the above state. We now define the unitaries

$$U_I=\sum_i^d|i\rangle\langle i|_S\otimes(U_i)_{A_1}, \tag{D7}$$

$$U_J=\sum_j^d|j\rangle\langle j|_S\otimes(U_j)_{A_2}, \tag{D8}$$

$$U=U_JU_I, \tag{D9}$$

where $\{U_i\}_{i=1}^d$, $\{U_j\}_{j=1}^d$ are unitary operator bases for $\mathcal{H}_{A_1}$ and $\mathcal{H}_{A_2}$, respectively, and $I=\{|i\rangle\}_{i=1}^d$ and $J=\{|j\rangle\}_{j=1}^d$

are any two mutually unbiased bases (MUBs) for $\mathcal{H}_S$; that is, they are both orthonormal and

$$|\langle i|j\rangle|^2 = \frac{1}{d}, \quad \forall\ i,j. \tag{D10}$$

In prime power dimension, there are known to exist sets of $d+1$ many of such MUBs, but there exist at least two in any dimension [30].

By direct evaluation, we now have

$$\mathrm{tr}_{A,B}[U(\rho\otimes|\phi^+\rangle\langle\phi^+|)U^\dagger] \tag{D11}$$

$$= \sum_{i,i',j,j'} |j\rangle\langle j|i\rangle\langle i|\rho|i'\rangle\langle i'|j'\rangle\langle j'|\mathrm{tr}(U_i U_{i'})\mathrm{tr}(U_j U_{j'})/d \tag{D12}$$

$$= \sum_j \mathrm{tr}(\rho)\frac{1}{d}|j\rangle\langle j| = \mathbb{I}_d, \tag{D13}$$

where we use both the orthonormality of the operator bases and the defining property of the MUBs.

We now turn to the unitary V. The construction is very similar to that of U. In fact, we use the fact that, for any unitary U,

$$(U\otimes\bar{U})|\phi_i^+\rangle = |\phi_i^+\rangle, \tag{D14}$$

where the bar denotes complex conjugation. We therefore define

$$V_I = \sum_i^d |i\rangle\langle i|_S \otimes (\bar{U}_i)_{B_1}, \tag{D15}$$

$$V_J = \sum_j^d |j\rangle\langle j|_S \otimes (\bar{U}_j)_{B_2}, \tag{D16}$$

$$V = V_I V_J, \tag{D17}$$

so that the unitaries now act on Bob's half of the entanglement. Equation (D4) then follows again by straightforward evaluation.

Finally, consider the case that d is not a square number. e is by construction always the smallest square number larger than, or equal to, d, so that we can always perform the splitting in Eq. (D5) in such a way that the resulting entangled states provide sufficient local randomness to perform the two dephasing operations. ∎

The above can now be used to construct an ideal PQC, as shown in the following.

Lemma 12 (Ideal private quantum channels).—With the notation from the previous lemma, the maps

$$\mathcal{X}(\cdot) := U(\cdot)U^\dagger, \tag{D18}$$

$$\mathcal{Y}(\cdot) := V(\cdot)V^\dagger \tag{D19}$$

form an ideal private quantum channel with key $|\Psi\rangle_K = |\phi^+\rangle$.

Proof.—The ideal reliability of the above construction follows immediately from Eq. (D4). The ideal security follows from the fact that every map $\mathcal{R}$ with the property that it completely randomizes a given system,

$$\mathcal{R}(\rho) = \mathbb{I}_d, \quad \forall\ \rho\in\mathcal{S}(\mathcal{H}_S), \tag{D20}$$

completely destroys all correlations that this system may have had with other systems [20], in the sense that, for any extension ρ_{SE} of some ρ,

$$\|(\mathcal{R}\otimes\mathrm{id})\rho_{SE} - \mathbb{I}_d\otimes\rho_E\|_1 = 0. \tag{D21}$$

But since $\mathrm{tr}_K\circ\mathcal{X}$ has this property, by Eq. (D3), Eq. (D21) implies ideal security in the sense of Eq. (D1). ∎

We now turn to a discussion of the properties of the above PQC. To begin with, note that it is catalytic in the sense that, in the absence of eavesdropping, the entanglement is, at the end, returned back in its original state. This follows from Eq. (D4). Especially since entanglement is commonly considered an expensive resource, this is a very appealing feature, even though it is not very robust, as we discuss in the next section.

Secondly, our PQC construction is optimal when considered as a noisy process, in the sense that it is impossible to construct an ideal PQC with less entanglement than we do, provided the global evolution is unitary. As in the case of the lower bounds for the dephasing map, discussed in Appendix A, we prove this optimality with respect to approximate PQCs, in order to show that our results are robust against slight deviations from an ideal PQC. To do so, we call, in analogy to the classical PQC, Eq. (38), a private quantum channel with key $|\Psi\rangle_K$ ϵ reliable, if, instead of Eq. (D1), it satisfies

$$\sup_{\rho_{S,E}\in\mathcal{S}(\mathcal{H}_S\otimes\mathcal{H}_E)} \|\mathrm{tr}_K\circ(\mathcal{X}\otimes\mathrm{id}_{K_B E})(\rho_{SE}\otimes|\Psi\rangle\langle\Psi|_K) - \tau\otimes\rho_E\|_1 \leq \epsilon. \tag{D22}$$

Lemma 13.—Let $(\mathcal{X},\mathcal{Y})$ be an ϵ-reliable private quantum channel with key $|\Psi\rangle_K$ for a quantum system of dimension d. If $\mathcal{X}$ is a unitary channel, then there exists an ϵ_{cr} such that, for all $\epsilon<\epsilon_{cr}$,

$$\dim(\mathcal{H}_A) \geq \max\{4, d^{1-\epsilon}\epsilon^{\epsilon/2}\}. \tag{D23}$$

Proof.—The proof is fully analogous to the discussion of the quantum case in Appendix A. We therefore give only a sketch. We have that $\mathrm{tr}_{K_B}(|\Psi\rangle_K) = \mathbb{I}_{d_A}$. Hence, ϵ reliability

together with the fact that $\mathcal{X} = U \cdot U^\dagger$ for some unitary operator U implies that the encoding channel on S is a quantum noisy operation $\mathcal{E}_Q^{d_A}$ as defined in Eq. (2). This further implies that $\tau = \mathbb{I}_d$, since the von Neumann entropy is nondecreasing under noisy operations and the channel has to work for the input state $\mathbb{I}_d$. We now bound d_A by considering a specific transition. Let $|\Psi\rangle_{SE}$ be the maximally entangled state over SE, where we choose the extension $\mathcal{H}_E$ to be a copy of $\mathcal{H}_S$. For this particular transition, ϵ reliability of the channel implies that

$$\|\mathcal{E}_Q^{d_A} \otimes \mathrm{id}_E(|\Psi\rangle\langle\Psi|_{SE}) - \mathbb{I}_d \otimes \mathbb{I}_d\|_1 \leq \epsilon. \quad \text{(D24)}$$

By Fannes's inequality, this implies

$$S[\mathcal{E}_Q^{d_A} \otimes \mathrm{id}_E(|\Psi\rangle\langle\Psi|_{SE})] \geq \log d^2 + \epsilon \log(\epsilon/d^2). \quad \text{(D25)}$$

We now consider the bipartition of the system SEA into SE and A. Using the Lieb-Araki inequality and following, from here on, exactly the same reasoning as that of Appendix A below Eq. (A8), yields the desired bound. ∎

1. Error correction, authentication, key recycling

As noted above, a particularly convenient feature of our PQC construction is that it is catalytic. This property implies that, in the absence of eavesdropping, the quantum key can be fully recycled. However, it is of course the basic premise of cryptography that one is not guaranteed the absence of eavesdropping. It is therefore natural to ask how robust our PQC implementation is to eavesdropping, by asking the following questions. Can Alice and Bob correct errors inflicted by an eavesdropper? How well can Alice and Bob check whether eavesdropping has occurred? How much of the key can Alice and Bob reuse in case they detect eavesdropping?

In this section, we show that Alice and Bob can use additional ebits to error correct, authenticate efficiently, and recycle part of the key even when eavesdropping occurs. The results of this section are mostly a translation of the arguments and techniques of Ref. [25] applied to our protocol.

a. Error correction

We first turn to the question of error correction. Consider, for simplicity, the case that Alice and Bob want to transmit a pure 2-qubit state vector $|\phi\rangle$ along our PQC construction (i.e., the setting depicted in Fig. 5). Following the results in the previous section, $|\phi\rangle$ can be sent using two ebits in the Bell state vector,

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle), \quad \text{(D26)}$$

as a key. We consider the effect of any Pauli error $P_i \in \{\mathbb{1}, X, Y, Z\}^{\otimes 2}$ that may have occurred during transmission of the data. The reason for this is that the most general effect of eavesdropping on the encoded state $\mathbb{I}_d = \mathrm{tr}_K \circ \mathcal{X}(|\phi\rangle\langle\phi|)$ that is sent between Alice and Bob can be described by a quantum channel $\mathcal{E}$ with decomposition

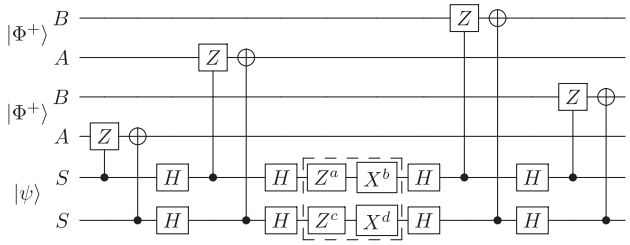


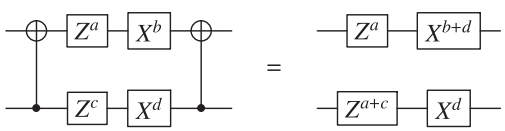
FIG. 6. The full entanglement-assisted PQC for a 2-qubit state with Pauli matrices chosen as unitary operator basis and dephasing in the computational and Pauli X eigenbases.

$$\mathcal{E}(\rho') = \sum_{i,j=0}^{15} e_{i,j} P_i \rho' P_j^\dagger. \quad \text{(D27)}$$

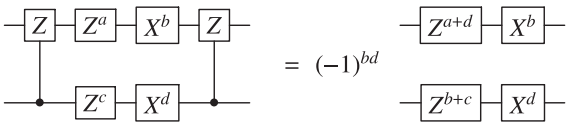
Hence, if there exists a measurement using local operations with classical communication (LOCC) that lets Alice and Bob perfectly distinguish between any two Pauli errors without destroying the state, then they can decorrelate the message from an eavesdropper and also error correct the message [25].

We now turn to show that there exist choices for the unitary operator basis and MUBs in the PQC of Lemma 12 such that Alice and Bob can discriminate any two Pauli error without destroying the transmitted state. This possibility arises because Alice and Bob can choose the encoding in such a way that there exists a one-to-one correspondence between Pauli errors and the final state of the entanglement they used for transmission. For this correspondence to arise it suffices to (a) use the unitary operator basis defined in Eq. (C1) as bases $\{U_i\}$ and $\{U_j\}$ in the construction of the unitaries U and V and (b) choose $I = \{|0\rangle, |1\rangle\}$ and $J = \{|+\rangle = H|0\rangle, |-\rangle = H|1\rangle\}$, where H is the Hadamard gate. For these choices, the total transmission process is given by Fig. 6, as a circuit diagram. Here, possible errors are given by the dashed box, with Alice's encoding to the left and Bob's decoding to the right of the dashed box and where we ignore global phases (for example, identifying $Y \equiv XZ$) since they do not alter the outcome.

Using the relations



and



together with the properties of entangled states, we find that a Pauli error $P(a,b,c,d)$ described by the tuple $(a,b,c,d) \in \{0,1\}^{\times 4}$ yields the final state vector,

$$(X^c Z^a)_{A_1} \otimes (X^{a+d} Z^b)_{A_2} |\Phi^+\rangle_{A_1 B_1} |\Phi^+\rangle_{A_2 B_2} P(a,b,c,d)|\psi\rangle, \tag{D28}$$

ignoring global phases and omitting identity operators. This implies that we can identify the tuple (a,b,c,d) exactly just by distinguishing the Bell states, since no two different Pauli errors produce the same pair of Bell states, establishing the required correspondence. The same holds true also for mixed state messages, by linearity of quantum mechanics, and it also straightforwardly generalizes to the case of larger messages, since we can think of such messages as being sent in chunks of size 2 using the above procedure.

Going back to the case $n = 2$, the above establishes a one-to-one correspondence between the 16 possible Pauli errors on the ciphertext and the 16 possible combinations of Bell state vectors:

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|0,0\rangle \pm |1,1\rangle), \tag{D29}$$

$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|0,1\rangle \pm |1,0\rangle). \tag{D30}$$

If Alice and Bob could discriminate between these 16 combinations using LOCC measurements, then by the above this would mean that they can both decorrelate the decoded state from an eavesdropper as well as perform error correction. However, this is not possible without the help of additional entanglement, since it is already impossible to discriminate between the four Bell states of a single ebit using LOCC measurements without further resources [31]. However, the situation is different if Alice and Bob have access to additional ebits. In particular, let $|\chi\rangle \in \{|\Phi^\pm\rangle, |\Psi^\pm\rangle\}$ be an unknown Bell state vector. Then, if Alice and Bob share an auxiliary ebit prepared in the state vector $|\Phi^+\rangle$, they can each apply a CNOT gate, controlling on the auxiliary sytem A and targeting S, which has the effect

$$\begin{aligned}
|\Phi^+\rangle_A |\Phi^+\rangle_S &\to |\Phi^+\rangle_A |\Phi^+\rangle_S, \\
|\Phi^+\rangle_A |\Phi^-\rangle_S &\to |\Phi^-\rangle_A |\Phi^-\rangle_S, \\
|\Phi^+\rangle_A |\Psi^+\rangle_S &\to |\Phi^+\rangle_A |\Psi^+\rangle_S, \\
|\Phi^+\rangle_A |\Psi^-\rangle_S &\to |\Phi^-\rangle_A |\Psi^-\rangle_S.
\end{aligned} \tag{D31}$$

If Alice and Bob now each measure their share of A in the Pauli X basis and their share of S in the Pauli Z basis and broadcast their measurement results, they can perfectly identify $|\chi\rangle$. Using this procedure for both ebits, they can extract full information about the error on the system and correct accordingly.

In summary, we have shown that Alice and Bob can perfectly discriminate between any two Pauli errors inflicted on the ciphertext during transmission, with the help of additional n ebits. In this way, however, our PQC construction loses the advantage in resources over that of Ref. [25], where error correction is also possible using $2n$ ebits in total.

b. Authentication and key recycling

The above error-correcting procedure has two disadvantages: Firstly, it requires a doubling of the total entanglement and, secondly, all the entanglement gets destroyed in the process. A more resource-effective strategy of Alice and Bob is to attempt to check for the occurrence of eavesdropping, destroying as little entanglement as possible, and consequently repeat the sending of the message while reusing as much of the entanglement as possible. We now discuss such a strategy in the asymptotic case, that is, when Alice and Bob send an n-qubit quantum message ρ_S using n ebits, in the limit $n \to \infty$.

Let $\mathbf{v}$ be a $2n$-bit string encoding the final state of the n ebits, with

$$|\Phi^+\rangle \to 00, \quad |\Psi^+\rangle \to 01, \quad |\Phi^-\rangle \to 10, \quad |\Psi^-\rangle \to 11,$$

and the first two bits corresponding to the first ebit, etc. In order to check for the occurrence of eavesdropping, Alice and Bob can employ a LOCC protocol constructed in Ref. [32] that yields the parity of any substring in $\mathbf{v}$, by destroying only a single ebit. Applying this protocol to r random substrings of $\mathbf{v}$, one has

$$\text{Prob}(\mathbf{v} \neq 00\ldots00 | \text{even parity in all } r \text{ rounds}) = \frac{1}{2^{-r}}.$$

Since $\mathbf{v} = 00\ldots00$ corresponds to the case in which no Pauli error occurred, this implies that in case Alice and Bob measure no odd parity, they know that the message has been successfully transferred and that they can reuse their ebits for future communication, with exponentially small probability of mistake and at the cost of vanishingly few ebits. Now, in case they detect odd parity for any of their r rounds, Alice and Bob consider the transfer unsuccessful

and attempt to recycle as many of their ebits as possible. This amounts to estimating $\mathbf{v}$ while destroying as few ebits as possible in the course of doing so. We can directly apply a key recycling procedure presented in Ref. [25] to our construction to achieve an asymptotic key recycling rate of $[1 - H(\delta)]$, where H is the binary Shannon entropy and $\delta > 0$ is a security parameter. We refer the reader to Ref. [25] for details.

These results should be compared with key recycling rates for the case of classical keys. There, the achievable recycling rates depend strongly on whether the message to be sent is classical (see, e.g., Refs. [33–35]) or quantum (see, e.g., Refs. [21,22,36]), and also on the possible attack scenarios that are being considered (see Refs. [21,22] for a discussion). Overall, however, the recycling rates can be considerably higher than those obtained here, albeit with significantly more complicated authentication schemes. Improving the recycling rates in the case of quantum keys thus remains an interesting open problem.

APPENDIX E: QUANTUM EXPANDERS

In this appendix, we discuss efficient approximate pinching to the main diagonal of an d-dimensional quantum system, of suitable dimension d, and provide the proof of Theorem 3. The proof of this statement is rooted in insights into random walks on expander graphs, is connected to properties of Wigner functions of discrete Weyl systems, and makes use of basic properties of quantum channels. It start from and builds upon the construction presented in Ref. [27], which in turn derives from the classical description in Ref. [29]. The latter work discusses a random walk on an expander graph featuring the vertex set $\mathbb{Z}_e^2$, so an $e \times e$ integer lattice. Reference [29] continuous to show that the random walk it constructs converges exponentially quickly to the uniform distribution $\mathbf{1}_{\mathbb{Z}_e^2}$ on this vertex set. Specifically, it is shown that there exists a doubly stochastic matrix such that for any probability distribution P on $\mathbb{Z}_e^2$, one has

$$\|S^k(P) - \mathbf{1}_{\mathbb{Z}_e^2}\|_2 \leq \frac{5\sqrt{2}}{8}\|S^{k-1}(P) - \mathbf{1}_{\mathbb{Z}_e^2}\|_2, \tag{E1}$$

for $k \geq 1$ being an integer. Here, the action of the doubly stochastic map acting upon a distribution on $\mathbb{Z}_e^2$ is written as $S(P)$. On $v = (v_p, v_q)^T \in \mathbb{Z}_e^2$, this doubly stochastic matrix originates from random affine transformations, drawn uniformly from the following eight transformations,

$$v \mapsto T_1 v, \quad v \mapsto T_2 v, \quad v \mapsto T_1 v + e_1, \quad v \mapsto T_2 v + e_2, \tag{E2}$$

and the four inverse transformations, with

$$T_1 := \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \qquad T_2 := \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \tag{E3}$$

and

$$e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{E4}$$

The graph underlying this construction, with the $e \times e$ lattice as vertex set, is an expander graph. Such an expander graph is usually referred to as an $(e^2, 8, \lambda)$ expander graph with $\lambda \leq 5\sqrt{2}/8$, in that it has e^2 vertices, each of which having 8 neighbors in the graph. The matrix S is sparse in that each row has 8 entries only. Clearly, the above implies that

$$\|S^k(P) - \mathbf{1}_{\mathbb{Z}_e^2}\|_2 \leq \sqrt{2}\left(\frac{5\sqrt{2}}{8}\right)^k. \tag{E5}$$

The prefactor of $\sqrt{2}$ originates from the fact that for any probability distribution P on $\mathbb{Z}_e^2$, one has

$$\begin{aligned} \|P - \mathbf{1}_{\mathbb{Z}_d^2}\|_2 &\leq [(1 - 1/e^2) - (e^2 - 1)/e^2]^{1/2} \\ &= \sqrt{2}(e^2 - 1)/e^2 \\ &\leq \sqrt{2}. \end{aligned} \tag{E6}$$

We relate this dimension e, which is left open at this point, to the physical dimension d of the quantum system subsequently.

The construction in a significantly altered setting will require some preparation. For this, we turn to discussing the phase space $d \times d$ for the d-dimensional quantum system with odd d. In the convention of Refs. [27,37], for phase space coordinates $(p, q) \in \mathbb{Z}_d^2$, the discrete Wigner function W_M of an operator M acting in Hilbert space can be written as

$$W_M(p, q) = \frac{1}{d}\mathrm{tr}[w(p, q)\Pi w(p, q)^\dagger M], \tag{E7}$$

where $(p, q) \mapsto w(p, q)$ is the family of Weyl operators and Π is the parity operator. The Weyl operators are composed of shift and clock operators, so the X and Z generalized Pauli matrices defined in Eqs. (19) and (22), respectively. Any affine transformation A, the linear part of which having a unit determinant on phase space coordinates $a \in \mathbb{Z}_d^2$, is unitarily reflected in Hilbert space as

$$W_{U_A \rho U_A^\dagger}(a) = W_\rho(A^{-1}(a)). \tag{E8}$$

Wigner functions are normalized as

$$\sum_{(p,q)\in\mathbb{Z}_d^2} W_\rho(p,q) = 1 \tag{E9}$$

for quantum states ρ. We treat Wigner functions for an operator M as matrices $W_M \in \mathbb{C}^{d\times d}$, with real-valued matrices for Hermitian M. A first well-known insight is stated here as a separate lemma for completeness.

Lemma 14 (Quantum states and Wigner functions).—For two quantum states ρ and σ on a Hilbert space $\mathcal{H}_S$ of dimension d associated with Wigner functions W_ρ, $W_\sigma : \mathbb{Z}_d^2 \to \mathbb{R}$, one has

$$\|\rho-\sigma\|_2^2 = \|W_\rho - W_\sigma\|_2^2 = \sum_{(p,q)\in\mathbb{Z}_d^2} [W_\rho(p,q) - W_\sigma(p,q)]^2. \tag{E10}$$

Proof.—This statement follows directly from the property that the Hilbert-Schmidt scalar product is inherited as

$$\mathrm{tr}(\rho\sigma) = \sum_{(p,q)\in\mathbb{Z}_d^2} W_\rho(p,q) W_\sigma(p,q), \tag{E11}$$

as follows from the analogous property of the characteristic function, and the definition of the 2-norm. ∎

The main insight of Ref. [27] is to acknowledge that random walks on integer lattices that are expander graphs can be connected to random unitary channels acting in Hilbert space that inherit the mixing properties from the classical random walk, by resorting to a phase space picture. The construction of Ref. [27] builds upon the random walk on the Margulis expander graph [29], the vertex set of which is $\mathbb{Z}_e^2$ for some e (here taken to be different from d, as it will take a different role subsequently). This random walk can be unitarily realized in quantum systems: In fact, the random walk follows directly from a convergence of a Wigner function, a function that shares all properties of a probability distribution, except being positive. Following the construction of the random walk on the expander graph, the quantum Margulis expander can be seen as a random unitary map,

$$\rho \mapsto \mathcal{D}(\rho) = \frac{1}{8}\sum_{j=1}^{8} U_j \rho U_j^\dagger, \tag{E12}$$

of Kraus rank 8 with suitable unitary $\{U_i\}$ with the property that

$$\|\mathcal{D}(\rho) - \mathbb{I}_e\|_2 \le \frac{5\sqrt{2}}{8}\|\rho - \mathbb{I}_e\|_2. \tag{E13}$$

A second insight on discrete Wigner functions that we will make use of is the following.

Lemma 15 (Wigner functions of pinched quantum states).—For any quantum state ρ on $\mathcal{H}_S$ of dimension d, the Wigner function of $\pi(\rho)$ satisfies

$$W_{\pi(\rho)}(p,q) = W_{\pi(\rho)}(p',q), \tag{E14}$$

for all $q, p, p' = 1, \ldots, d$.

Proof.—This statement follows directly from the definition of Wigner functions. ∎

This means that Wigner functions of pinched states are constant along the first coordinate. Prepared in this fashion, we can finally turn to the new construction. This construction of a random unitary channel will deviate from this construction in a significant way: We identify for each $q \in \mathbb{Z}_d$ for $d = e^2$ the entire line $\{(p,q) \in \mathbb{Z}_d^2\}$ of the $(d \times d)$-dimensional phase space as a vectorized $e \times e$ lattice, on which the above affine maps act. The property of the unit determinant of the linear part in the affine mapping is preserved. In fact, it will act in precisely the same way on each line simultaneously, by applying one of the 8 affine transformations defined in Eqs. (E2)–(E4). This gives rise to 8 affine maps on $\mathbb{Z}_d^2$. Acting on Wigner functions, this process can again be realized as a random unitary channel,

$$\rho \mapsto \mathcal{T}(\rho) = \frac{1}{8}\sum_{j=1}^{8} V_j \rho V_j^\dagger, \tag{E15}$$

with unitaries $\{V_i\}$. Clearly, the entire Wigner function W_ρ of a state is normalized according to Eq. (E9). We refer to

$$x_q := \sum_{p\,\in\,\mathbb{Z}_d} W_\rho(p,q) \tag{E16}$$

as the weight of each column. We now discuss the convergence properties of the above random unitary channel. For an integer $k \ge 1$, we have

$$\begin{aligned}\|\mathcal{T}^k(\rho) - \pi(\rho)\|_2^2 &= \|W_{\mathcal{T}^k(\rho)} - W_{\pi(\rho)}\|_2^2 \\ &= \sum_{q\,\in\,\mathbb{Z}_d} x_q^2 \sum_{p\,\in\,\mathbb{Z}_d} \left(\frac{W_{\mathcal{T}^k(\rho)}(p,q)}{x_q} - \frac{1}{d}\right)^2,\end{aligned} \tag{E17}$$

treating each columns separately. Using $x_q \le d$ for all q and using a worst-case bound for all q gives

$$\|\mathcal{T}^k(\rho) - \pi(\rho)\|_2^2 \le d^3 \sum_{p\in\mathbb{Z}_d} \left(\frac{W_{\mathcal{T}^k(\rho)}(p,q)}{x_q} - \frac{1}{d}\right)^2, \tag{E18}$$

and following Eq. (E5), one obtains

$$\|\mathcal{T}^k(\rho) - \pi(\rho)\|_2^2 \le 2d^3 \left(\frac{5\sqrt{2}}{8}\right)^{2k}. \tag{E19}$$

In this way, we arrive at the anticipated result, by embedding the random unitary system into an explicit quantum model, in the nomenclature of the main text.

[1] G. Gour, M. P. Mueller, V. Narasimhachar, R. W. Spekkens, and N. Y. Halpern, *The Resource Theory of Informational Nonequilibrium in Thermodynamics*, Phys. Rep. **583**, 1 (2015).

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

[3] N. Linden, S. Popescu, A. J. Short, and A. Winter, *Quantum Mechanical Evolution towards Thermal Equilibrium*, Phys. Rev. E **79**, 061103 (2009).

[4] W. H. Zurek, *Decoherence, Einselection, and the Quantum Origins of the Classical*, Rev. Mod. Phys. **75**, 715 (2003).

[5] E. Joos, H. D. Zeh, C. Kiefer, D. J. W. Giulini, J. Kupsch, and I.-O. Stamatescu, *Decoherence and the Appearance of a Classical World in Quantum Theory* (Springer, Berlin, 2003).

[6] A. S. Holevo, *Statistical Structure of Quantum Theory* (Springer, Berlin, 2001).

[7] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).

[8] A. Ambainis, M. Mosca, A. Tapp, and R. De Wolf, *Private Quantum Channels*, in *Proceedings of the 41st Annual Symposium on Foundations of Computer Science*, (IEEE Computer Society, 2000), pp. 547–553.

[9] P. O. Boykin and V. Roychowdhury, *Optimal Encryption of Quantum Bits*, Phys. Rev. A **67**, 042317 (2003).

[10] M. P. Mueller, *Correlating Thermal Machines and the Second Law at the Nanoscale*, arXiv:1707.03451.

[11] A. W. Marshall, I. Olkin, and B. C. Arnold, *Inequalities: Theory of Majorization and Its Applications* (Springer, New York, 2011).

[12] A. Horn, *Doubly Stochastic Matrices and the Diagonal of a Rotation Matrix*, Am. J. Math. **76**, 620 (1954).

[13] J. Scharlau and M. P. Mueller, *Quantum Horn's Lemma, Finite Heat Baths, and the Third Law of Thermodynamics*, Quantum **2**, 54 (2018).

[14] J. Schwinger, *Unitary Operator Bases*, Proc. Natl. Acad. Sci. U.S.A. **46**, 570 (1960).

[15] R. F. Werner, *All Teleportation and Dense Coding Schemes*, J. Phys. A **34**, 7081 (2001).

[16] D. Jonathan and M. B. Plenio, *Entanglement-Assisted Local Manipulation of Pure Quantum States*, Phys. Rev. Lett. **83**, 1455 (1999).

[17] N. H. Y. Ng, L. Mancinska, C. Cirstoiu, J. Eisert, and S. Wehner, *Limits to Catalysis in Quantum Thermodynamics*, New J. Phys. **17**, 085004 (2015).

[18] J. Eisert and M. Wilkens, *Catalysis of Entanglement Manipulation for Mixed States*, Phys. Rev. Lett. **85**, 437 (2000).

[19] A. Ambainis, J. Bouda, and A. Winter, *Nonmalleable Encryption of Quantum Information*, J. Math. Phys. (N.Y.) **50**, 042106 (2009).

[20] P. Hayden, D. Leung, P. W. Shor, and A. Winter, *Randomizing Quantum States: Constructions and Applications*, Commun. Math. Phys. **250**, 371 (2004).

[21] C. Portmann, *Quantum Authentication with Key Recycling*, in *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques* (Springer, New York, 2017), pp. 339–368.

[22] P. Hayden, D. W. Leung, and D. Mayers, *The Universal Composable Security of Quantum Message Authentication with Key Recyling*, arXiv:1610.09434.

[23] If instead of the diamond norm a PQC's security is defined with respect to the weaker trace norm, then any unitary 1-design provides an ideal channel and there exist both randomized [20] and deterministic [24] constructions of PQCs that require only $n + O[\log(n)]$ many bits of shared key.

[24] A. Ambainis and A. Smith, *Small Pseudo-Random Families of Matrices: Derandomizing Approximate Quantum Encryption*, in *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques. RANDOM 2004, APPROX 2004*, Lecture Notes in Computer Science (Springer, Berlin, Heidelberg, 2004).

[25] D. W. Leung, *Quantum Vernam Cipher*, Quantum Inf. Comput. **2**, 14 (2002).

[26] M. B. Hastings, *Random Unitaries Give Quantum Expanders*, Phys. Rev. A **76**, 032315 (2007).

[27] D. Gross and J. Eisert, *Quantum Margulis Expanders*, Quantum Inf. Comput. **8**, 722 (2008).

[28] A. W. Harrow, *Quantum Expanders from Any Classical Cayley Graph Expander*, Quantum Inf. Comput. **8**, 715 (2008).

[29] G. A. Margulis, *Explicit Constructions of Concentrators*, Prob. Peredachi Inf. **9**, 71 (1973).

[30] I. Bengtsson and K. Życzkowski, *Geometry of Quantum States: An Introduction to Quantum Entanglement*, 2nd ed. (Cambridge University Press, Cambridge, England, 2017).

[31] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, *Local Distinguishability of Multipartite Orthogonal Quantum States*, Phys. Rev. Lett. **85**, 4972 (2000).

[32] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, *Mixed-State Entanglement and Quantum Error Correction*, Phys. Rev. A **54**, 3824 (1996).

[33] C. H. Bennett, G. Brassard, and S. Breidbart, *Quantum Cryptography II: How to Re-Use a One-Time Pad Safely Even if* P = NP, Nat. Comput. **13**, 453 (2014).

[34] I. Damgard, T. B. Pedersen, and L. Salvail, *A quantum cipher with near optimal key-recycling*, in *CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara*, Lecture Notes in Computer Science, Vol. 3621 (Springer, New York, 2005), pp. 494–510.

[35] S. Fehr and L. Salvail, *Quantum Authentication and Encryption with Key Recycling*, in *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques* (Springer, New York, 2017), pp. 311–338.

[36] J. Oppenheim and M. Horodecki, *How to Reuse a One-Time Pad and Other Notes on Authentication, Encryption, and Protection of Quantum Information*, Phys. Rev. A **72**, 042309 (2005).

[37] D. Gross, *Hudson's Theorem for Finite-Dimensional Quantum Systems*, J. Math. Phys. (N.Y.) **47**, 122107 (2006).