Limitations for private randomness repeaters

Karol Horodecki,[1,2] Ryszard P. Kostecki,[1] Roberto Salazar,[1] and Michał Studziński[3]

[1]*National Quantum Information Centre in Gdańsk and Institute of Informatics, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, 80-952 Gdańsk, Poland*

[2]*International Centre for Theory of Quantum Technologies, University of Gdańsk, 80-952 Gdańsk, Poland*

[3]*National Quantum Information Centre in Gdańsk and Institute of Theoretical Physics and Astrophysics, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, 80-952 Gdańsk, Poland*

(Received 17 March 2020; accepted 19 June 2020; published 16 July 2020)

Cryptographic protocols are often based on the two main resources: private randomness and private key. In this paper, we develop the relationship between these two resources. First, we show that any state containing perfect, directly accessible, private key (a private state) is a particular case of the state containing perfect, directly accessible, private randomness (an independent state). We then demonstrate a fundamental limitation on the possibility of transferring the privacy of random bits in quantum networks with an intermediate repeater station. More precisely, we provide an upper bound on the rate of repeated randomness in this scenario, similar to the one derived for private key repeaters. This bound holds for states with positive partial transposition. We further demonstrate the power of this upper bound by showing a gap between the localizable and the repeated private randomness for separable Werner states. In the case of restricted class of operations, we provide also a bound on repeated randomness which holds for arbitrary states.

DOI: 10.1103/PhysRevA.102.012615

I. INTRODUCTION

Ensuring the security of communication in quantum internet is one of the main current challenges of quantum technology [1]. In this context, two distant honest parties must distribute a secure key, i.e., a private correlated string of bits. A prominent security framework that assures the distribution of encrypted bits in a quantum network is the *quantum repeaters* scheme [2–5]. It allows for distributing secure key employing pure maximally entangled states [6] and entanglement swapping [2,3].

In a recent article [7] the paradigm of network key swapping was extended to the most general scenario of private states [8,9], that are, generally, mixed quantum states. A striking result of [7] is the existence of mixed states ρ and ρ', such that no protocol between three parties $A, B, C = C_1C_2$ can transfer a non-negligible amount of key between A and B from the key shared between the parties AC_1 and BC_2.

This fact shows an intriguing property of the secure key extracted from mixed quantum states: it is not transitive for an arbitrary state, i.e., the fact that A has secure connection with C and C has secure connection with B does not imply that A can establish secure connection with B.

In this article, we investigate the network properties of another critical resource for cryptography: the private randomness. In most cases, it is used for testing a quantum device or postprocessing the classical outcome of the latter. For this reason, the privacy of randomness appears as a precondition for secure key distribution. This resource was recognized quite early (for the review on this topic, see [10]; the framework for single-party private randomness extraction was developed in [11]), and has motivated commercial implementations (e.g., Ref. [12]). Only recently a resource theory framework of (distributed) private randomness has been established [13] (see, e.g., Refs. [6,14] for a review of other resource theories). According to this approach, the task of distillation of private randomness amounts to obtaining the so-called independent states α via closed local operations and dephasing channel (CLODCC). More precisely the CLODCC operations are compositions of (i) local unitary operations by each of the honest parties (U_A and U_B) and (ii) communication via dephasing channel from A to B and vice versa. The dephasing channel transfers the state measured in a fixed (say computational) basis. These operations were introduced in the context of purity distillation. The choice of this class of operations in resource theory of private randomness is justified, as these operations do not bring in private randomness.

It is common in the literature to represent the private randomness obtained by two honest parties against an eavesdropper in terms of tripartite states $(\sum_{i=0}^{d_A-1} \frac{1}{d_A}|i\rangle\langle i|) \otimes \sum_{k=0}^{d_B-1} \frac{1}{d_B}|k\rangle\langle k|) \otimes \rho_E$ (here ρ_E is representing an arbitrary state of the eavesdropper). In such an approach the honest parties are using local operations and public communication. However, it is shown in [13] that this approach is equivalent to distilling specific bipartite states—the independent states, by means of CLODCC operations. The independent states have a form of coherence "twisted" into a shared mixed state:

$$\alpha_{d_A,d_B} = \sum_{i,j,k,l} |i\rangle\langle j| \otimes |k\rangle\langle l| \otimes U_{ik}\sigma_{A'B'}U_{jl}^{\dagger}, \tag{1}$$

as it can be written in the following way:

$$\tau|+\rangle\langle+|_A \otimes |+\rangle\langle+|_B \otimes \sigma_{A'B'}\tau^{\dagger}, \tag{2}$$

with $|+\rangle_{A/B} = \sum_{i=0}^{d_{A/B}-1} \frac{1}{\sqrt{d_{A/B}}}|i\rangle$ and $\tau = \sum_{ij} |ij\rangle\langle ij| \otimes U_{ij}^{A'B'}$.

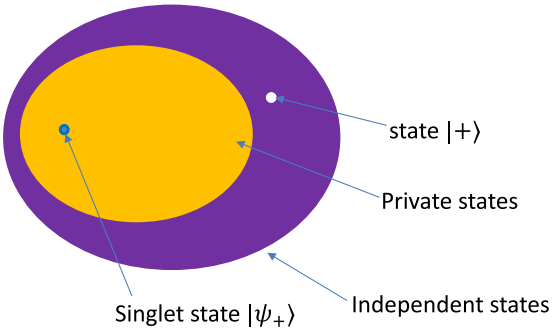

FIG. 1. Onion structure of quantum states containing ideal privacy. The singlet state is an example of a private state. The set of private states is a proper subset of the set of independent states. The state $|+\rangle$ is an independent state, which is not a private state.

In the scenario considered here, i.e., when two parties want to localize private randomness at one place, we will be interested in local independent states:

$$\alpha_{d_A} = \sum_{i,j} |i\rangle\langle j| \otimes U_i \sigma_{A'B'} U_j^\dagger. \tag{3}$$

Although the structural analogy between the theories of private key and randomness is somewhat natural, the results explicitly determining this relation are missing. Developing this analogy, we first show that any state containing an ideal private key (a private state) [8,9] is, in fact, an independent state. We therefore prove that the sets of quantum states containing ideal privacy form an onion structure (see Fig. 1).

We then demonstrate that private randomness exhibits the similar type of limitation as a secure key when distributed on a communication network [7]. The answer to the question "Can one always swap private randomness of general mixed quantum states?" follows this close analogy.

The conceptual description that we introduce to capture the topology of security in the network is called the loyalty network. It represents each party as a vertex, while a directed edge from vertex A to vertex B represents A being secure due to loyalty of B. In the weaker sense, loyalty $A \to B$ means that A trusts that B will not hand over his subsystem ρ_B of the shared joint state ρ_{AB} to any eavesdropper Eve. Clearly, if B is not loyal to A, the local private randomness of A is equal to localizable purity. However, we will assume a stronger sense of loyalty, in which loyal B cooperates in favor of A, such that A has access to as much private randomness of a state ρ_{AB} as it is possible (part of it is obtained from the correlations between A and B).

We will exemplify this concept with entanglement swapping of the singlet $|\psi\rangle_+^{AB} := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}$:

$$|\psi\rangle_+^{AC_1} \otimes |\psi\rangle_+^{C_2B} \xrightarrow{\text{ent. swap.}} |\psi\rangle_+^{AB}. \tag{4}$$

This operation can be interpreted as follows.

Initially, party A has 1 bit of private randomness due to the loyalty of party $C = (C_1C_2)$, and party C has 1 bit of private randomness due to the loyalty of party B. After applying entanglement swapping, party A has 1 bit of private randomness due to the loyalty of party B, and does not need to rely on the loyalty of party C anymore.

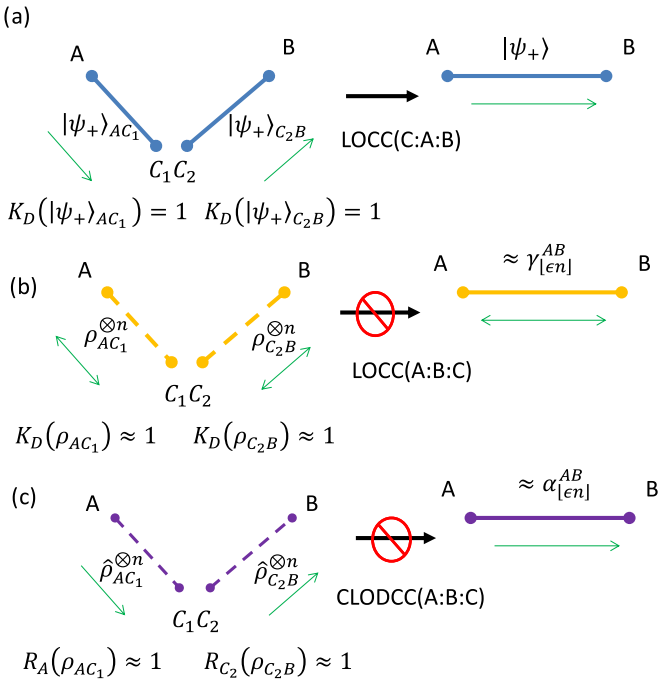

FIG. 2. Depiction of the limitation for private randomness in the context of network repeaters. Part (a) depicts redistribution of loyalty in the network via entanglement swapping: on the LHS A trusts C and C trusts B, as depicted by the green arrows. On the RHS A trusts B only [2]. Part (b) shows that for any $\epsilon > 0$ there exist states with positive partial transposition, that have almost 1 bit of secure key K_D each. However, there is no LOCC protocol between three parties that outputs an approximate private state with more than $\lfloor n\epsilon \rfloor$ bits of key [7]. Part (c) depicts the result of this paper, in analogy to the case (b): for any $\epsilon > 0$, there exist states that have almost 1 bit of private randomness, but there is no CLODCC protocol between three parties that outputs *an independent state* with more than $\lfloor n\epsilon \rfloor$ bits of private randomness.

Another way to see the dependencies in the loyalty network of (4) is as follows: at the beginning A trusts C and B trusts C, while the task is to remove C out of the network and to make A trust B (or B trust A). As we show in Sec. IV, the bound for repeated private randomness which we provide is invariant under the swap; hence it covers also this particular topology of network. Moreover, in Sec. VII we show that there are swap-invariant states (e.g., some Werner states) that exhibit gap between localizable and repeated private randomness.

We then ask if such transformation is possible for all mixed quantum states, when the number n of copies of initial states goes to infinity,

$$(\rho_{AC_1} \otimes \tilde{\rho}_{C_2B})^{\otimes n} \xrightarrow[n\to\infty]{\text{priv. rand. repeater?}} \alpha_{k\times n}^{AB}, \tag{5}$$

where $k \times n$ is the rate of private randomness that can be obtained via tripartite operations from n copies of the input state in the form of the independent states. These states, denoted by α, contain ideal private randomness directly accessible by local complete von Neumann measurement on the subsystem of α. For the qualitative summary of the results, see Fig. 2 and Sec. I A.

Since we adopt methods shown in [7], the upper bound that we obtain works for the states with positive partial transposition (PPT states). These are bipartite states ρ that satisfy $[\mathbb{I}\otimes(\cdot)^\top](\rho)\geqslant 0$ [15], where $(\cdot)^\top$ is a transposition and $\mathbb{I}$ is an identity operator. We show the power of the upper bound by inspecting the gap between localizable and repeated private randomness for separable Werner states. These are states interpolating between symmetric and antisymmetric states. Within the range of interpolating parameter that guarantees separability, for sufficiently large local dimension d, we observe the presence of a gap. We also consider a strictly smaller class of operations, generated by compositions of (i) n optimal single copy operations among the three parties, followed by (ii) distillation by A and B solely, via general CLODCC($A:B$) operations. For this class, we derive a bound for repeated private randomness for arbitrary states. We then exemplify it by providing a family of states that do not have positive partial transposition, yet exhibit the same gap (of almost 1) between localizable and repeated randomness.

A. Summary of the main results

For the reader's convenience, we summarize here the main results of our contribution.

Here and further in this paper we write interchangeably $\rho_{AC_1}, \tilde{\rho}_{C_2B}$ and $\rho,\tilde{\rho}$ whenever it is clear from the context. Given a state ρ_{AB}, $S(A)_\rho$ will denote the von Neumann entropy of subsystem A of ρ_{AB}, $S(A)_\rho := -\mathrm{Tr}(\rho_A\log_2\rho_A)$, with $\rho_A=\mathrm{Tr}_B\rho_{AB}$. By $S(A|B)_\rho$ we denote the conditional entropy $S(AB)_\rho - S(A)_\rho$, while $I(A:B)_\rho = S(A)_\rho + S(B)_\rho - S(AB)_\rho$ is the quantum mutual information. By $\log_2|A|$ we mean the log of dimension of the system A (similarly for B and AB). In case it is necessary, we will explicitly write the state of which dimension is invoked: $\log_2|A|_\rho$. The logarithm is of the base 2 throughout all of this paper. For the special case of a distribution $\{p,(1-p)\}$, its Shannon entropy we denote as $h(p)=-p\log_2 p-(1-p)\log_2(1-p)$. We also refer to it as the binary Shannon entropy.

The main step towards our results is the definition of the repeated randomness $\mathcal{R}_A^{A\leftrightarrow C_1C_2\leftrightarrow B}(\rho\otimes\tilde{\rho})$ (an analog of repeated key), which is the asymptotic rate ($n\to\infty$) of private randomness (in the form of the ibits) that can be achieved by the three parties from initial n copies of the state $\rho\otimes\tilde{\rho}$ via operations allowed in the resource theory of private randomness [13] (called CLODCC). Separately, we define the private randomness repeater rate in the i.i.d. case, i.e., when three parties perform the same CLODCC operation on each of the copies of the state, followed by a general operation from CLODCC($A:B$).

As the main result, we prove the following upper bound on the rate of repeated private randomness:

$$\mathcal{R}_A^{A\leftrightarrow C_1C_2\leftrightarrow B}(\rho_{AC_1}\otimes\tilde{\rho}_{C_2B}) \leqslant D\left(\rho^\Gamma||\frac{\mathbb{I}}{|AC_1|}\right)+D\left(\tilde{\rho}^\Gamma||\frac{\mathbb{I}}{|C_2B|}\right), \tag{6}$$

where $D(\rho||\sigma)=\mathrm{Tr}(\rho\log_2\rho-\rho\log_2\sigma)$ is the quantum relative entropy and $\rho^\Gamma := (\mathbb{I}\otimes T)(\rho)$ denotes the partial transposition of ρ. The right-hand side (RHS) of (6) can be quite small in some cases, as we show with particular examples of states for which repeated private randomness is negligible. It can be rephrased in terms of the global purity, $G(\rho_{XY}) := \log_2|XY| - S(XY)_\rho$, as

$$\mathcal{R}_A^{A\leftrightarrow C_1C_2\leftrightarrow B}(\rho_{AC_1}\otimes\rho_{C_2B}) \leqslant G\left(\rho^\Gamma_{AC_1}\right)+G\left(\tilde{\rho}^\Gamma_{C_2B}\right). \tag{7}$$

The above form of the bound would be natural in the purity distillation paradigm [16]. In the context of private randomness distillation it will be also natural to rephrase it in terms of correlations, i.e., quantum mutual information. This is because the mutual information quantifies the nontrivial (not equivalent to purity) amount of private randomness. For the case when $\rho=\tilde{\rho}$ has positive partial transposition and has both subsystems in maximally mixed states, we have immediate corollary.

The partial transposition does not change the entropy of either of the subsystems of ρ. One subsystem (say A) is the same after applying the map $\mathbb{I}_A\otimes(\cdot)_B^\top$. For the other, by the fact that $\det(X)=\det(X^\top)$ one has $\det(\rho_B-\lambda\mathbb{I})=\det(\rho_B-\lambda\mathbb{I})^\top=\det(\rho_B^\top-\lambda\mathbb{I})$. Hence the roots of this polynomial, which are the eigenvalues of ρ_B, are the same as for $\rho_B^\top$:

$$\mathcal{R}_A^{A\leftrightarrow C_1C_2\leftrightarrow B}\left(\rho_{AC_1}\otimes\rho_{C_2B}\right)\leqslant 2I(A:C_1)_{\rho^\Gamma}. \tag{8}$$

This stems from the fact that the quantum relative entropy between a state and the product of its two subsystems is equal to quantum mutual information between them.

The key result of [13] which allows us to interpret our main result is the protocol of optimal private randomness distillation. It determines how a single party can localize as much of the private randomness in her system as possible. Additionally, in [13] it is shown that there are two sources of private randomness: local, in the form of purity, and shared, in the form of correlations. This fact is supported by quantitative result: the amount of localized private randomness of a state with positive partial transposition ρ_{AC_1} in the asymptotic limit reads

$$\begin{aligned}R_A(\rho_{AC_1}) = {}& [\log_2|A| - S(A)_\rho] + [\log_2|C_1| - S(C_1)_\rho] \\ & + I(A:C_1)_\rho.\end{aligned} \tag{9}$$

Thus the amount of locally achievable private randomness for the ρ_{AC_1} (i.e., between A and C_1) is equal to the sum of local purity $\log_2|A|-S(A)_\rho$ and the amount of correlation in the shared state (i.e., the quantum mutual information). When the state ρ has subsystems in a maximally mixed state, we can use the bound from Eq. (8) since no local purity can be achieved, i.e., $R_A(\rho_{AC_1})=I(A:C_1)_\rho$. It applies for states with positive partial transposition, for which there is a gap:

$$I(A:C_1)_\rho > 2I(A:C_1)_{\rho^\Gamma}. \tag{10}$$

Although we notice the gap between correlations of ρ and ρ^Γ for states having key (and therefore distillable private randomness) [17], the above gap cannot be demonstrated in the same way as in [7] due to the factor 2 above. Instead, since the key is not the only local form of private randomness, we study the most famous single parameter class of states—the Werner states. In particular, we observe that the symmetric Werner state [18], $\rho_s^d=\frac{1}{d^2+d}(\mathbb{I}+V)$, where $V :=$

$\sum_{i,j} |ij\rangle\langle ji|$ is called a swap operator, satisfies

$$I(A:B)_{\rho_s^d} = 1 + \log_2\left(\frac{d}{d+1}\right) \xrightarrow[d\to\infty]{} 1,$$

$$I(A:B)_{(\rho_s^d)^\Gamma} = \frac{1}{d}\log_2 d + \frac{d-1}{d}\log_2\frac{d}{d-1} \xrightarrow[d\to\infty]{} 0.$$

Hence, for large dimensions of d,

$$R_A\left(\rho_s^d\right) \approx 1, \quad \mathcal{R}_A\left(\rho_s^d \otimes \rho_s^d\right) \approx 0. \tag{11}$$

As we show in Sec. VII, any separable Werner state of sufficiently high dimension exhibits the gap, as it is the case for the symmetric one. This result is analogous to the limitation for key repeaters shown in [7]. In contrast, however, it is achieved on separable states, rather than on the approximate private states used in [7].

Finally, we consider a variant of the i.i.d. case, when the three parties are forced to use identical operations on each copy of the state and, further, A and B apply any CLODCC($A:B$) on such obtained outputs. For a particular independent state of the form

$$\alpha_{V,d} = \frac{1}{2}\begin{bmatrix} \frac{\mathbb{I}}{d^2} & \frac{V}{d^2} \\ \frac{V}{d^2} & \frac{\mathbb{I}}{d^2} \end{bmatrix}, \tag{12}$$

we prove the existence of a gap between private randomness $R_A(\alpha_{V,d})$, $R_B(\alpha_{V,d})$ and i.i.d. repeated private randomness $\mathcal{R}_A^{\text{iid}}(\alpha_{V,d})$, whenever dimension is sufficiently large. Namely, we prove that, for $d > 32$, we have $R_A(\alpha_{V,d}) = R_B(\alpha_{V,d}) = 1$, while $\mathcal{R}_A^{\text{iid}}(\alpha_{V,d}) < 1$. In particular, for $d > 11$, we have

$$\mathcal{R}_A^{\text{iid}}(\alpha_{V,d}) \leqslant \frac{4\log_2 d}{d} + \eta\left(\frac{4}{d}\right), \tag{13}$$

which clearly goes to zero when $d \to \infty$.

Our paper is organized as follows. We start from Sec. II, where all necessary tools are presented; in particular, we introduce the concepts of the CLODCC operations and of a local idit. In Sec. II A we precisely describe the framework in which we work, stating what the involved parties are allowed to perform. We do so by defining the allowed class of operations (CLODCC) and its distinguished subclass, and by establishing relations between them. Section III analyzes the relationship between the sets of private states and of independent states, showing they are not equal to each other. This finding distinguishes our work from previous results on limitations on quantum key repeaters. Section IV is divided into two separate parts. In the first one, we prove results on the state discrimination from the maximal noise by using CLODCC operations. In the second part, we derive our main result: an upper bound on the rate of repeated randomness. This implies existence of the states with localizable randomness equal to 1 that have vanishingly small repeated independent randomness. In Sec. V we provide alternative proof of the bound on repeated private randomness for states with positive partial transposition, showing, as a by-product, that the latter rate is bounded by a value computed on partially transposed states. In Sec. VI, we present the limitation for a private randomness repeater in the i.i.d. case, where parties first perform the same CLODCC operation on each copy of the state and then apply arbitrary CLODCC on these copies. In particular, for a chosen class of independent states and for sufficiently large dimension, we show a gap between the private randomness and the repeated private randomness. In Sec. VII we show a broad class of Werner states for which our main result holds. We close this paper with Sec. IX, summarizing our main results and putting them in the broader picture of possible further research.

II. PRELIMINARIES ON PRIVATE RANDOMNESS AND KEY

In this section, we recall necessary concepts of the resource theory of private randomness and private key, allowing the reader to better understand our further results.

The free operations of this theory are closed operations and classical communication via dephasing channel (CLODCC). This class of operations is a subclass of the well-known LOCC operations, and was introduced as free operations in the resource theory of purity [19]. The systems under consideration are closed, only local unitary transformations are allowed, and the honest parties can exchange subsystems through a dephasing channel. Such dephasing channel can be realized by an eavesdropper Eve via (1) attaching an ancillary pure state $|0\rangle_E$ to each system M passing between the honest parties, (2) performing a CNOT (controlled-NOT) gate (with source at M and target at the system E), and (3) collecting E in some quantum memory.

The target states (i.e., states containing ideal private randomness in a directly accessible form) are given by independent states [13], which can be viewed as the result of twisting of coherent states [20] $\frac{1}{\sqrt{d}}(\sum_{i=0}^{d-1}|i\rangle_A) \otimes \frac{1}{\sqrt{d}}(\sum_{i=0}^{d-1}|i\rangle_B)$. In the case of two dits of private randomness the independent states have the form

$$\alpha_{ABA'B'} := U|+\rangle\langle+|_A \otimes |+\rangle\langle+|_B \otimes \sigma_{A'B'} U^\dagger, \tag{14}$$

where $U = \sum_{i,j}|ij\rangle\langle ij| \otimes U_{ij}$ and U_{ij} is a unitary transformation for each ij.

By local idit we will mean the independent state given in Eq. (14) when $|A| = d$ and $|B| = 1$ (or $|A| = 1$ and $|B| = d$). Hence private randomness can be directly accessed from a part of such state that is localized either at A or at B. To explicitly indicate the number m of private random bits directly accessible via measuring systems A (or B) in a local idit, we will denote it as α_m.

Note that these states are similar in construction to the private states, defined [8,9] by *twisting* of maximally entangled states $|\psi\rangle_+^{AB} := \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|ii\rangle_{AB}$,

$$\gamma_{ABA'B'} := U|\psi\rangle_+\langle\psi|_{AB} \otimes \sigma_{A'B'} U^\dagger, \tag{15}$$

with the unitary operator $U = \sum_i |ii\rangle\langle ii| \otimes U_i$. Every key distillation protocol ends up in states approximating private states, while every protocol which distills private randomness produces approximated independent states. In Sec. III we show that any private state is an independent state.

Following [13], $R_A(\rho)$ will denote the private randomness localizable on system A by means of CLODCC($A:B$) operations from (asymptotically many) copies of ρ_{AB}.

An important result from [13] asserts the following: if a bipartite state has a negative conditional entropy, then the

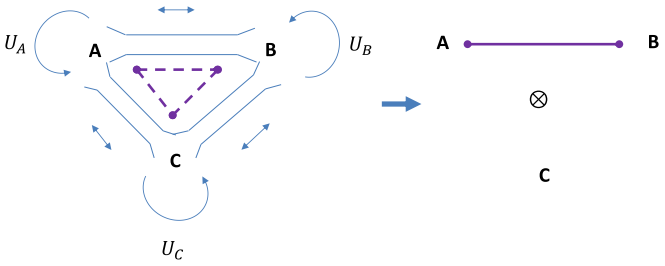

FIG. 3. Depiction of the considered scenario. All three parties can perform locally unitary transformations, and can send a system down a dephasing channel to the other parties. Their task is to distill *independent states* shared by A and B.

whole of its private randomness content can be localized at each of the parties by means of CLODCC operations.

Theorem 1 (Corollary from Theorem 4 of [13]). Any bipartite state ρ_{AB} satisfying $S(B|A)_\rho > 0$ satisfies $R_A(\rho_{AB}) = \log_2 |AB| - S(AB)_\rho$.

The quantity $\log_2 |AB| - S(AB)_\rho$ is called a global purity [19], and is also a trivial upper bound on the amount of localizable private randomness (achieved when both parties can operate globally on the system AB). Any separable state and, in general, states with positive partial transposition have positive quantum conditional entropy (i.e., negative coherent information) [6]. Moreover, as we will see, some ibits that have negative partial transposition share this property with PPT states. Furthermore, the resource theory of private randomness has an empty set of free states: adding a maximally mixed state can increase the amount of localizable private randomness. However, the maximally mixed state on its own represents the set of states which are closed under CLODCC operations (see Sec. IV) and it contains zero localizable private randomness. We can, therefore, view this state as a correspondent of the set of separable states in the resource theory of private key.

In what follows $\rho \approx_\epsilon \rho'$ denotes $||\rho - \rho'||_1 \leqslant \epsilon$ with $||X||_1 := \mathrm{Tr}|X|$ for a Hermitian operator X.

A. Scenario of private randomness repeaters

In our scenario, there are three involved parties: A, B, and C. Party C has two subsystems: C_1 and C_2. A dephasing channel connects each pair of parties. Each of the parties can perform either (i) unitary operation or (ii) sending of a system to some of the other parties (or both of them). We denote as CLODCC$(A : C_1C_2 : B)$ the class of operation generated by arbitrary (possibly infinite) compositions of the above operations. The parties are given (arbitrarily large) n copies of input states ρ_{AC_1} and ρ_{C_2B} shared by A and C, and C and B, respectively. The task of the parties is to obtain a local idit α_m on systems A and B with the largest possible amount m of bits of private randomness, with randomness directly accessible by von Neumann measurement on Alice's system [see part (c) of Fig. 2 and Fig. 3]. In the case of the above scenario, we obtain the bound for states with positive partial transposition.

To obtain analogous results for states that are not having positive partial transposition, we will consider a much simpler scenario, with a smaller class of allowed operations, CLODCC$[C^{\mathrm{iid}} : (A^{\mathrm{iid}} : B^{\mathrm{iid}})] \subsetneq$ CLODCC$(A : B : C)$. For the case of n copies of the input states, this class is defined by the composition of two operations, denoted as $(C : A : B)^{\mathrm{iid}}$ and $A \leftrightarrow B$, respectively. The former operation corresponds to an action of the three parties: they behave identically on each copy, producing n copies of the best single-round output $\hat{\rho}$. The latter operation refers to A and B performing a general CLODCC$(A : B)$ operation on $\hat{\rho}^{\otimes n}$. The task for the parties is again to distill independent states shared by A and B.

We end this section with several simple observations, which are crucial for our later considerations.

Observation 1. There is CLODCC$(A : C_1C_2 : B) \subset$ CLODCC$(C_1C_2 : AB)$.

Proof. The difference between these two sets of operations is that A and B are joining their labs. They can now perform global unitary transformations, and we have to show that they still are able to dephase parts of their system. For example, A can send a state to B via a dephasing channel according to definition of the set of CLODCC$(A : C_1C_2 : B)$ (and vice versa). When A and B acting together want to dephase some system, they can send it to C who sends it back to them. The claim is then seen from the fact that a single dephasing channel between C and AB can also simulate two separate dephasing channels between C and A, and C and B, respectively, while operations of C are the same in both sets. ■

Consider the set S of operations on system AB induced from the operations in CLODCC$(C : AB)$ via composing the latter with a partial trace over system C. We will argue that this set includes operations that are a composition of unitary transformations and projections in the computational basis. We will denote the set of all such compositions as U + Deph.

Observation 2. The set S of transformations of system AB defined as $\mathrm{Tr}_C \Lambda_{C:AB}(\rho_{ABC})$, with $\Lambda_{C:AB} \in$ CLODCC$(C : AB)$, satisfies U + Deph $\subset S$.

Proof. It follows directly from the fact that operations $U_{AB} \otimes \mathbb{I}_C$ and $\{P_a \otimes \mathbb{I}_C\}$ with a being a subsystem of AB belong to the set CLODCC$(C : AB)$. Indeed, the von Neumann measurement on a subsystem of AB can be realized via composition of sending the measured system a to C and resending it back to AB. The same holds for arbitrary composition of the latter two. The assertion then follows from the fact that $\mathrm{Tr}_C(L_{AB} \otimes \mathbb{I}_C)(\rho_{ABC}) = L_{AB}(\mathrm{Tr}_C \rho_{ABC})$ for any completely positive trace preserving linear map L_{AB}. ■

It is common that the allowed operations in a given resource theory preserve the set of the free states, i.e., transform any free state into a free state. The observation below implements this property for the resource theory of (distributed) private randomness.

Observation 3. Every $\Lambda \in$ CLODCC is unital, i.e., Λ preserves the maximally mixed state.

Proof. According to the definition of CLODCC, presented in Sec. II, operations in this class are composed of unitary operations and dephasing together with sending the dephased system from one party to another. Clearly, the first two operations preserve the maximally mixed state. The only nonunital operation is sending of the dephased system. However, a subsystem of a maximally mixed state is also a maximally mixed one; hence the map outputs also a maximally mixed state, but (possibly) of different dimension on systems A, B, and

C (denoted as $|\hat{A}|$, $|\hat{B}|$, and $|\hat{C}|$, respectively). However, $|A| + |B| + |C| = |\hat{A}| + |\hat{B}| + |\hat{C}|$, because the CLODCC class does not contain the partial trace operation. Hence this map can be seen as "redistributing" the maximally mixed state among the three systems. ■

III. PRIVATE STATES ARE INDEPENDENT STATES

In this section, we discuss the differences between private states and independent states. In particular, we prove that the set of independent states is strictly included in the set of all private states. This follows from the fact that there are product states, such as $|+\rangle \otimes \mathbb{I}/2$, which are ibits having zero distillable key, because entanglement is a precondition for secure key [21]. Nevertheless, the techniques used here are related to those in [7]. For example, the relative entropy is taken with respect to the set of separable states, while here it is taken with respect to the maximally mixed state. We have to simplify the approach, because the private randomness is zero for the maximally mixed state, and is nonzero for any other state. We show that these two similar, although different, classes of states are related by the strict inclusion $PS \subsetneq IS$, which is the main result of this section.

Proposition 1. Any private state is a (local) independent state, while the converse statement is not valid in general, $PS \subsetneq IS$. Moreover, the private random bit can be located at either of the parties.

Proof. Any private state has a form $\gamma_{ABA'B'} = \sum_{i,j=0}^{d-1} \frac{1}{d} |ii\rangle\langle jj| \otimes U_i \sigma_{A'B'} U_j^\dagger$. The twisting involved in the definition of any private state can be simplified to have a single control [22]:

$$\gamma_{ABA'B'} = \left(\sum_{i=0}^{d-1} |i\rangle\langle i|_A \otimes \mathbb{I}_B \otimes U_i\right) |\psi_+\rangle\langle\psi_+|_{AB} \otimes \sigma_{A'B'} \times \left(\sum_{j=0}^{d-1} |j\rangle\langle j|_A \otimes \mathbb{I}_B \otimes U_j^\dagger\right). \tag{16}$$

It is then enough to express the singlet state $|\psi_+\rangle_{AB}$ as an output of a control-shift gate: $|\psi_+\rangle_{AB} = \tau|+\rangle_A \otimes |0\rangle_B$ with $|+\rangle = \sum_{i=0}^{d-1} \frac{1}{\sqrt{d}} |i\rangle$ and $\tau = \sum_i |i\rangle\langle i|_A \otimes S_{i,d}$, where $S_{i,d}|j\rangle = |j + i \bmod d\rangle$, if d is prime. If d is not prime, it can be expressed uniquely by multiplication of primes: $d = d_1 \times \cdots \times d_k$ where d_l is prime for $l \in \{1, \ldots, k\}$ (for the sake of uniqueness, we assume $d_l \leqslant d_{l'}$ for $l \leqslant l'$). In this case we define $\tau := \bigotimes_{l=1}^{k} (\sum_{i=0}^{d_l-1} |i\rangle\langle i| \otimes S_{i,d_l})$, where S_{i,d_l} is defined as above with d_l in place of d. Substituting this form of a private state into (16) immediately yields

$$\gamma_{ABA'B'} = \left[\sum_{i=0}^{d-1} |i\rangle\langle i|_A \otimes \left(\bigotimes_{l=1}^{k} S_{l[i],d_l}\right) \otimes U_i\right] |+\rangle\langle+|_A \otimes |0\rangle \times \langle 0|_B \otimes \sigma_{A'B'} \left[\sum_{j=0}^{d-1} |j\rangle\langle j|_A \otimes \left(\bigotimes_{l=1}^{k} S_{l[j],d_l}^\dagger\right) \otimes U_j^\dagger\right], \tag{17}$$

where $l[i]$ is the lth digit of i written in a multibase system of k bases: $d_1, \ldots, d_k$. Written in such a form, this state is by definition a (local) independent state. Indeed, consider Eq. (14), with substitution B of system of dimension 1 and B' system in state $|0\rangle\langle 0| \otimes \mathrm{Tr}_{A'}\sigma$. The strictness of inclusion follows from the state $|+\rangle \otimes \mathbb{I}/2$ being an ibit, while having no distillable key, because entanglement is a precondition of security [21]. Because the singlet state is swap invariant, the same reasoning follows when one expresses it as $|\psi_+\rangle_{AB} = \tau'|+\rangle_B \otimes |0\rangle_A$ with τ' having control at B rather than at A. This fact shows that the private random bit can be located in any of the parties. ■

The above Theorem implies the onion structure of quantum states containing ideal privacy: $|\psi_+\rangle \in PS \subsetneq IS$ and $|+\rangle \in IS \setminus PS$ (see Fig. 1).

IV. LIMITATIONS ON PRIVATE RANDOMNESS REPEATERS

The main result of this section provides a bound on repeated independent randomness. It is based on the restricted relative entropy bound of the Supplemental Material of [7], with the difference that allowed operations are taken to be CLODCC instead of LOCC, while the set of free states is given by a maximally mixed state, instead of the set of separable states. We will first describe the asymptotic distinguishability using operations from CLODCC.

A. Discriminating states from maximal noise via CLODCC operations

We are interested in an asymptotic distinguishability. In analogy to the restricted relative entropy of entanglement of [23], we consider now the simplest of the restricted relative entropy: the relative entropy with respect to the maximally mixed state. Due to limitations of the specific technique, our results hold only for states with positive partial transposition (PPT states). We build on the results of [7].

Definition 1. For a bipartite state on $\mathcal{H} := \mathbb{C}^d \otimes \mathbb{C}^d$, the restricted relative entropy distance from the maximal mixed state achievable via operations from set S of POVMS is

$$D_S(\rho) := \sup_{\Lambda_M \in S} D\left[\Lambda_M(\rho) || \Lambda_M\left(\frac{\mathbb{I}}{d^2}\right)\right], \tag{18}$$

$$D_S^\infty(\rho) := \lim_{n\to\infty} \frac{1}{n} D_S(\rho^{\otimes n}), \tag{19}$$

where $\Lambda_M := \sum_i \mathrm{Tr}_{\mathcal{H}}[M^i(\cdot)]|i\rangle\langle i|$ is a completely positive trace-preserving map, $n \in \mathbb{N}$, and $D(\cdot||\cdot)$ is the Kullback-Leibler relative entropy of two probability distributions. A restriction of S in (18) and (19) to the set J, corresponding to such Λ_M that belong to the CLODCC class, defines $D_J(\rho)$ and $D_J^\infty(\rho)$, respectively.

Theorem 2. If ρ is a density operator on $\mathcal{H} := \mathbb{C}^d \otimes \mathbb{C}^d$, $\Gamma := \mathrm{id}_{\mathbb{C}^d} \otimes (\cdot)^\top$, and $X^\Gamma := \Gamma(X)$ for a linear bounded $X : \mathcal{H} \to \mathcal{H}$, then

$$\rho^\Gamma \geqslant 0 \Rightarrow D_J^\infty(\rho) \leqslant D\left(\rho^\Gamma || \frac{\mathbb{I}}{d^2}\right). \tag{20}$$

Proof. Let $\Lambda \in \mathrm{CLODCC}$ and let $\{|i\rangle\langle i|\}$ be a base in $\mathcal{H}$. Then

$$\begin{aligned}\sup_{\Lambda\in\mathrm{CLODCC}} D\left[\Lambda(\rho^{\otimes n})||\Lambda\left(\frac{\mathbb{I}^{\otimes n}}{d^{2n}}\right)\right] &:= \sup_{\Lambda\in\mathrm{CLODCC}} D\left[\sum_i \mathrm{Tr}_{\mathcal{H}}\left(M^i_\Lambda \rho^{\otimes n}\right)\otimes|i\rangle\langle i|\Big|\Big|\sum_i \mathrm{Tr}_{\mathcal{H}}\left(M^i_\Lambda \frac{\mathbb{I}^{\otimes n}}{d^{2n}}\right)\otimes|i\rangle\langle i|\right]\\ &= \sup_{\Lambda\in\mathrm{CLODCC}} D\left[\sum_i \mathrm{Tr}_{\mathcal{H}}\left[\left(M^i_\Lambda\right)^\Gamma(\rho^\Gamma)^{\otimes n}\right]\otimes|i\rangle\langle i|\Big|\Big|\sum_i \mathrm{Tr}_{\mathcal{H}}\left(\left(M^i_\Lambda\right)^\Gamma \frac{\mathbb{I}^{\otimes n}}{d^{2n}}\right)\otimes|i\rangle\langle i|\right]\\ &\leqslant D\left[(\rho^\Gamma)^{\otimes n}||\left(\frac{\mathbb{I}}{d^2}\right)^{\otimes n}\right] = nD\left(\rho^\Gamma||\frac{\mathbb{I}}{d^2}\right). \end{aligned} \tag{21}$$

Hence

$$\lim_{n\to\infty}\frac{1}{n}\sup_{\Lambda\in\mathrm{CLODCC}} D\left[\Lambda(\rho^{\otimes n})||\Lambda\left(\frac{\mathbb{I}^{\otimes n}}{d^{2n}}\right)\right] \leqslant \lim_{n\to\infty} D\left(\rho^\Gamma||\frac{\mathbb{I}}{d^2}\right). \tag{22}$$

In the above $\Lambda = \{M_\Lambda\}$ is a POVM of an operation from the set CLODCC. In the second equality we use the identity $\mathrm{Tr}(XY) = \mathrm{Tr}(X^\Gamma Y^\Gamma)$ for matrices X and Y, and the fact that $(\rho^\otimes)^\Gamma = (\rho^\Gamma)^{\otimes n}$. The last inequality follows from the fact that the relative entropy is nonincreasing under CPTP maps. ■

B. Rate of repeated private randomness

Now we are in a position to derive an asymptotic version of the distinguishability bound, that is, the quantity that upper bounds the rate of repeated randomness $\mathcal{R}_A^{A\leftrightarrow C\leftrightarrow B}$. It measures the distinguishability of the state from the maximally mixed state in terms of the relative entropy of the probability distributions that can be obtained by CLODCC.

We start from presenting a rigorous definition of rates of repeated randomness. Namely, for input states ρ_{AC_1} between A and C, and $\tilde{\rho}_{C_2B}$ between C and B, we call

$$\begin{aligned}&\mathcal{R}_A^{A\leftrightarrow C\leftrightarrow B}(\rho_{AC_1}\otimes\tilde{\rho}_{C_2B})\\ &:= \inf_{\epsilon>0}\limsup_{n\to\infty}\sup_{\Lambda_n\in\mathrm{CLODCC},\alpha_m} \\ &\quad\times\left\{\frac{m}{n} : \mathrm{Tr}_C[\Lambda_n((\rho_{AC_1}\otimes\tilde{\rho}_{C_2B})^{\otimes n})] \approx_\epsilon \alpha_m\right\}\end{aligned} \tag{23}$$

the quantum private randomness repeater rate of ρ and $\tilde{\rho}$ with respect to arbitrary CLODCC operations among A, B, and C, that can be obtained on a system A.

Let $\mathrm{CLODCC}(A:B)$ be the set of POVMs which can be implemented with CLODCC operations. An element of this class is a corresponding CPTP map. That is, instead of a POVM given by $\{M_i\}$, we consider the CPTP map $M : X \mapsto \sum_i[\mathrm{Tr}(M_iX)]\otimes|i\rangle\langle i|$. Hence $M(\rho)$ is a distribution of POVM elements from the stet $\{M_i\}$ measured for a density operator ρ. Our bound on the quantum independent randomness repeater rate involves the measured relative entropy with respect to the set CLODCC,

$$\begin{aligned}&D_{C\leftrightarrow AB}(\rho_{AC_1}\otimes\tilde{\rho}_{C_2B})\\ &:= \sup_{M\in\mathrm{CLODCC}(C:AB)} D\left[M(\rho\otimes\tilde{\rho})\|M\left(\frac{\mathbb{I}}{d_{ABC}}\right)\right].\end{aligned} \tag{24}$$

By d_{ABC} we mean the multiplication of dimensions of ρ and $\tilde{\rho}$. We denote by $D^\infty_{C\leftrightarrow AB}$ the regularized version of (24), analogous to the relationship between (19) and (18).

Before we prove the bound, we need a lemma showing a lower bound on the measured relative entropy distance from the maximally mixed state for states that approximate independent states. We show that the measured relative entropy distance with respect to U + Deph from the maximally mixed state is proportional to m on $\rho \approx_\epsilon \alpha_m$.

Lemma 1. For $\rho \approx_\epsilon \alpha_m^{AA'B}$ of dimensionality $|AA'B|$, we have

$$D_{\mathrm{U+Deph}}\left(\rho\|\frac{\mathbb{I}}{|AA'B|}\right) \geqslant (1-\epsilon)m - h(\epsilon). \tag{25}$$

Proof. We will follow the proof of Lemma from [7] with appropriate changes, since a general idit is twisted coherence rather than entanglement. We use the fact that α_m can be expressed as $UP_A^m\otimes\sigma_{A'B'}U^\dagger$. Here U is a controlled unitary operator, with control A and target $A'B'$, while $\sigma_{A'B'}$ is an arbitrary state. Then,

$$\begin{aligned}&D_{\mathrm{U+Deph}}\left(\rho\|\frac{\mathbb{I}}{|AA'B|}\right)\\ &= \sup_{\Lambda\in\{\mathrm{U+Deph}\}} D\left(\{\mathrm{Tr}[M_\Lambda(\rho)]\}\Big\|\left\{\mathrm{Tr}\left[M_\Lambda\left(\frac{\mathbb{I}}{|AA'B|}\right)\right]\right\}\right)\\ &\geqslant D_{\mathrm{U+Deph}}\left[\mathrm{Tr}_{A'B'}(U\rho U^\dagger)\|\mathrm{Tr}_{A'B'}\left(U\frac{\mathbb{I}}{|AA'B|}U^\dagger\right)\right]\\ &= D_{\mathrm{U+Deph}}\left(\tilde{P}_A^m\|\frac{\mathbb{I}}{|A|}\right)\\ &\geqslant D_{\mathrm{U+Deph}}\left[\{\mathrm{Tr}\left(P_{m,F}\tilde{P}_A^m\right)\}\Big\|\left\{\mathrm{Tr}\left(P_{m,F}\frac{\mathbb{I}}{|A|}\right)\right\}\right]\\ &\geqslant (1-\epsilon)m - h(\epsilon),\end{aligned} \tag{26}$$

where $\tilde{P}_A^m := \mathrm{Tr}_{A'B'}(U\rho U^\dagger)$ is a state, ϵ close to $P_A^m \equiv \sum_{i,j=0}^{2^m-1}\frac{1}{2^m}|i\rangle\langle j|_A$. The first inequality holds due to monotonicity of $D(\cdot||\cdot)$ and the fact that $U\in\{\mathrm{U+Deph}\}$. The second inequality follows from (i) monotonicity under the projective measurement $\{P_{m,F}\}$ onto the basis of the Fourier transform of the basis $\{|i\rangle\}_{i=0}^{2^m-1}$ (P_m^A is an element of this transformed basis) and (ii) $P_{m,F}\in\{\mathrm{U+Deph}\}$. The last inequality is due to $\{\mathrm{Tr}(P_{m,F}\frac{\mathbb{I}}{|A|})\} = \{1/2^m\}$. Moreover, $\mathrm{Tr}(P_{m,F}\tilde{P}_m^A) \geqslant 1-\epsilon$, which follows from $\rho\approx_\epsilon\alpha_m$. Further, the highest entropy among distributions $\{1-\epsilon,\lambda_1,\ldots,\lambda_{d-1}\}$ is achieved by the most mixed one for $\lambda_i = \frac{\epsilon}{d-1}$. We thus obtain the lower bound on the relative entropy of the distribution, as claimed. ■

We now come to the main result of this section.

Theorem 3. For all states ρ_{AC_1} and $\tilde{\rho}_{C_2B}$:

$$\mathcal{R}_A^{A\leftrightarrow C\leftrightarrow B}(\rho_{AC_1}\otimes\tilde{\rho}_{C_2B}) \leqslant D^{\infty}_{C\leftrightarrow AB}(\rho_{AC_1}\otimes\tilde{\rho}_{C_2B}). \tag{27}$$

Proof. For any $\epsilon > 0$, by the definition of the rate of repeated private randomness, there exists $n\in\mathbb{N}$ and $\Lambda\in\beta := \mathrm{CLODCC}(A^n : C^n : B^n)$, such that $r \geqslant \mathcal{R}_A^{A\leftrightarrow C\leftrightarrow B}(\rho_{AC_1}\otimes\tilde{\rho}_{C_2B}) - \epsilon$ and $\tilde{\alpha} := \mathrm{Tr}_C\Lambda[(\rho_{AC_1}\otimes\tilde{\rho}_{C_BB})^{\otimes n}] \approx_\epsilon \alpha_{\lfloor nr\rfloor}$, where $\lfloor\cdot\rfloor$ denotes the floor function. Taking $\sigma_{ABC} = \frac{\mathbb{I}}{|ABC|}$ and $\tilde{\sigma} := \mathrm{Tr}_C\Lambda(\sigma)$, we have

$$\begin{aligned}
&\max_{M\in\beta} D\big[M\big(\rho_{AC_1}^{\otimes n}\otimes\tilde{\rho}_{C_2B}^{\otimes n}\big)\|M(\sigma_{ACB})\big]\\
&\quad\geqslant \max_{M\in\beta} D\big[M\big(\Lambda\big(\rho_{AC_1}^{\otimes n}\otimes\tilde{\rho}_{C_2B}^{\otimes n}\big)\big)\|M(\Lambda(\sigma_{ACB}))\big]\\
&\quad\geqslant \max_{M\in\mathrm{U+Deph}} D[M(\tilde{\alpha}_{AB})\|M(\tilde{\sigma}_{AB})].
\end{aligned}\tag{28}$$

Thanks to Observation 1 and the assumption that $\Lambda\in\mathrm{CLODCC}(C:AB)$ we obtain the first inequality. The third line follows from the fact that we restrict maximization to the set of operations that are induced on system AB from a $\mathrm{CLODCC}(C:AB)$ via trace over C. The set of these operations is denoted by S. Due to Observation 2, the set S includes U + Deph. We get the lower quantity if we restrict supremum to the operations from U + Deph $\subsetneq S$. Due to Observation 3, $\tilde{\sigma} = \frac{\mathbb{I}}{d_{\mathrm{out}}}$, where d_{out} is the dimension of the output of the map $\mathrm{Tr}_C\Lambda(\cdot)$.

Applying Lemma 1 with $\tilde{\alpha}\approx_\epsilon \alpha_{\lfloor nr\rfloor}$ we arrive at

$$\max_{M\in\mathrm{U+Deph}} D[M(\tilde{\alpha}_{AB})\|M(\tilde{\sigma}_{AB})] \geqslant (1-\epsilon)\lfloor nr\rfloor - h(\epsilon). \tag{29}$$

Bounds (28) and (29), together with minimization over σ and taking the limit $n\to\infty$, imply the following lower bound on $D^{\infty}_{C\leftrightarrow AB}$:

$$D^{\infty}_{C\leftrightarrow AB}(\rho_{AC_1}\otimes\tilde{\rho}_{C_2B}) \geqslant (1-\epsilon)r. \tag{30}$$

Taking into account that $r \geqslant \mathcal{R}_A^{A\leftrightarrow C\leftrightarrow B}(\rho_{AC_1}\otimes\tilde{\rho}_{C_2B}) - \epsilon$ with arbitrary ϵ, the statement is proved. ■

Corollary 1. The following inequality holds for all PPT states $\rho = \rho_{C_1A}$ and $\tilde{\rho} = \tilde{\rho}_{C_2B}$:

$$\mathcal{R}_A^{A\leftrightarrow C\leftrightarrow B}(\rho\otimes\tilde{\rho}) \leqslant D\left(\rho^\Gamma||\frac{\mathrm{I}}{|AC_1|}\right) + D\left(\tilde{\rho}^\Gamma||\frac{\mathrm{I}}{|C_2B|}\right), \tag{31}$$

where $d_\rho, d_{\tilde{\rho}}$ stand for the dimensions of ρ, $\tilde{\rho}$, respectively.

This Corollary follows from applying Theorems 2 and 3 to $J = \mathrm{CLODCC}(C:AB)$.

From the bound (31) in Corollary 1 we can conclude that there are states that have localizable randomness equal to almost 1, while their repeated independent randomness is vanishingly small (see Sec. VII for examples).

To interpret the above result, we should compare the localizable and repeated private randomness. Theorem 1 of [13], invoked in Sec. II, states that localizable private randomness of an input state ρ_{AC_1} is equal to its global purity, i.e., $\log_2|AC_1| - S(AC_1)_\rho$. Using the equality of $\log_2|AC_1|$ for ρ_{AC_1} and for $\rho^\Gamma_{AC_1}$, the RHS of (31) can be rewritten as $\log_2|AC_1| - S(AC_1)_{\rho^\Gamma} + \log_2|C_2B| - S(C_2B)_{\tilde{\rho}^\Gamma}$. However, for any state σ_{AC_1}, $\log_2|AC_1| - S(AC_1)_\sigma = [\log_2|A| - S(A)_\sigma] + [\log_2|C_1| - S(C_1)_\sigma] + I(A:C_1)_\sigma$. That is, the global purity can be split into purity accessible locally (sum of the first two terms), and the correlation part (the mutual information). The locally accessible purity is a type of private randomness that is accessible to A and B without help of C, and hence is always available in our private randomness repeater scenario. The partial transposition does not change entropy of the local subsystem, $S(A)_\rho = S(A)_{\rho^\Gamma}$, and the same holds for B. Hence, for $\tilde{\rho} = \rho$, the difference between localizable private randomness from ρ at system A and our bound reads

$$\begin{aligned}
&\log_2|AC_1| - S(AC_1)_\rho - [\log_2|AC_1| - S(AC_1)_{\rho^\Gamma}]\\
&\quad - [\log_2|C_2B| - S(C_2B)_{\tilde{\rho}^\Gamma}]\\
&= I(A:C_1)_\rho - [\log_2|B| - S(B)_{\tilde{\rho}} + \log_2|C_2| - S(C_2)_{\tilde{\rho}}\\
&\quad + I(A:C_1)_{\rho^\Gamma} + I(C_2:B)_{\tilde{\rho}^\Gamma}].
\end{aligned}\tag{32}$$

Thus, due to the term $\log_2|B| - S(B)_\rho + \log_2|C_2| - S(C_2)_\rho$ appearing on the RHS of (32), the above bound is weak for states that contain local purity. However, as we will see, it is sufficiently powerful for all states that have local purity equal to zero, i.e., that have both subsystems in maximally mixed states. In the latter case, considering also $\rho_{AC_1} = \tilde{\rho}_{C_2B}$, the gap between localizable and repeated localizable randomness reads $I(A:B)_\rho - 2I(A:B)_{\rho^\Gamma}$. In Sec. VII we will study behavior of this gap for the family of separable Werner states.

V. DIRECT BOUND FOR PPT STATES IS NOT TIGHTER THAN THE INDIRECT ONE

In this section we provide a more direct proof of Corollary 1. One might think that the latter bound could be improved by getting rid of the factor 2 in front of the one presented in (8) in Sec. I A, as analogous phenomenon happens for the private key (see Lemma 12 and Theorem 13 of the Supplemental Material of [7]). As we will see below, this is not the case: we obtain the same bound. We show it here, because its intermediate step is worth mentioning separately. It states that the repeated private randomness is upper bounded for states from PPT set by its value taken on the partially transposed state.

Theorem 4. For any two bipartite states ρ and $\tilde{\rho}$ that have positive partial transposition,

$$\mathcal{R}_A^{A\leftrightarrow C_1C_2\leftrightarrow B}(\rho_{AC_1}\otimes\tilde{\rho}_{C_2B}) \leqslant \mathcal{R}_A^{A\leftrightarrow C_1C_2\leftrightarrow B}\big(\rho^\Gamma_{AC_1}\otimes\tilde{\rho}^\Gamma_{C_2B}\big). \tag{33}$$

Proof. We first note that the definition of $\mathcal{R}_A^{A\leftrightarrow C\leftrightarrow B}$ involves the term $\mathrm{Tr}_C\Lambda[(\rho_{AC_1}\otimes\rho_{C_2B})^{\otimes n}]$, with $\Lambda\in\mathrm{CLODCC}(A:C:B)\subset\mathrm{LOCC}(A:C:B)\subset SEP(A:B:C)$, where $SEP(A:B:C)$ are the operations that can be expressed in a form $\sum_i A_i\otimes B_i\otimes C_i(\cdot)A_i^\dagger\otimes B_i^\dagger\otimes C_i^\dagger$. Adopting the idea of the proof of Lemma 12 from [7], we note that $\mathrm{Tr}_C(\sigma_{ACB}) = \mathrm{Tr}_C[(\mathbb{I}_{AB}\otimes T_C)\sigma_{ABC}]$, i.e., we can transpose the state on system C before tracing it, then trace and obtain the original state traced over system C. This fact holds for any state σ, and in particular for $\sigma := \Lambda(\rho_{AC_1}\otimes\tilde{\rho}_{C_2B})$. Hence

$$\begin{aligned}
&\mathrm{Tr}_C\Lambda[(\rho_{AC_1}\otimes\rho_{C_2B})^{\otimes n}]\\
&\quad = \mathrm{Tr}_C\{(\mathbb{I}_{AB}\otimes T_C)\Lambda[(\rho_{AC_1}\otimes\rho_{C_2B})^{\otimes n}]\}
\end{aligned}$$

$$= \mathrm{Tr}_C \Bigg((\mathbb{I}_{AB} \otimes T_C) \sum_{ijk} A_i \otimes B_j \otimes \times C_k (\rho_{AC_1} \otimes \rho_{C_2B})^{\otimes n} A_i^\dagger \otimes B_j^\dagger \otimes C_k^\dagger \Bigg). \quad (34)$$

Using $(\mathbb{I} \otimes T)(X_1 \otimes X_2 \rho Y_1 \otimes Y_2) = X_1 \otimes Y_2^T (\rho^\Gamma) Y_2 \otimes X_2^T$, we obtain

$$\begin{aligned} &\mathrm{Tr}_C \Bigg((\mathbb{I}_{AB} \otimes T_C) \sum_{ijk} A_i \otimes B_j \otimes \times C_k (\rho_{AC_1} \otimes \rho_{C_2B})^{\otimes n} A_i^\dagger \otimes B_j^\dagger \otimes C_k^\dagger \Bigg) \\ &= \mathrm{Tr}_C \Bigg(\sum_{ijk} A_i \otimes B_j \otimes C_k^* \big(\rho_{AC_1}^\Gamma \otimes \rho_{C_2B}^\Gamma\big)^{\otimes n} \times A_i^\dagger \otimes B_j^\dagger \otimes (C_k^*)^\dagger \Bigg). \end{aligned} \quad (35)$$

We will show now that C_k^* are such that the total operation $\sum_{ijk} A_i \otimes B_j \otimes C_k^*(\cdot) A_i^\dagger \otimes B_j^\dagger \otimes (C_k^*)^\dagger$ is a valid CLODCC($C : AB$) operation. Let $\hookrightarrow |0\rangle\langle 0|_X$ denote the operation of adding an ancillary state $|0\rangle$ to the system X. Any operation from CLODCC($C : AB$) can be simulated by the following four LOCC operations (and their composition in a proper order).

(1) Unitary transformation on system C: $U_{C \to C'c}$.

(2) Dephasing channel from C to A, i.e., $\{P_c^i \otimes \mathbb{I}_{C'}\}_{i=0}^{|c|-1}$ with $P^i := |i\rangle\langle i|_c$.

(3) Operation which changes the system c in a way that it is in the same state as some dephased system on AB. It first adds an ancillary blank state, and further performs appropriate shift $\{S_{i,|c|}^c\}_{i=0}^{|c|-1} \circ \hookrightarrow |0\rangle\langle 0|_c$, with $S_{i,|c|}^c |j\rangle := |j + i \bmod |c|\rangle$. This operation is controlled by the outcomes of $\{P_a^i \otimes \mathbb{I}_{\bar{a}}\}_{i=0}^{|a|-1}$ with $P_a^i := |i\rangle\langle i|_a$, a being an arbitrary subsystem of AB satisfying $|a| = |c|$ and $\bar{a}$ denoting complement of AB to a.

(4) Tr_c (used only after a dephasing channel and an operation on system A analogous to the third operation on this list).

For any k there is $C_k = M_1 \circ \cdots \circ M_l \circ \cdots$, where M_l are Kraus' operators from the above set of operations (up to the restriction that Tr_c can be used only after the third operation from the list). Hence $C_k^* = M_1^* \circ \cdots \circ M_l^* \circ \cdots$. All operations on the above list, apart from the first, do not change under complex conjugation, as they are formulated with real numbers, while $U_{C \to C'c}$ becomes another unitary transformation $U_{C \to C'c}^*$. Thus any CLODCC($C : AB$) operation Λ after partial transposition $(\cdot)_C^\top \otimes \mathbb{I}_{AB}$ becomes some other operation $\Lambda' \in$ CLODCC($C : AB$). By evaluating it on $\rho_{AC_1}^\Gamma \otimes \rho_{C_2B}^\Gamma$, the assertion follows. ■

Remark 1. Although the fact that CLODCC($A : B$) $\subsetneq$ LOCC($A : B$) was already noticed in the context of resource theory of purity [16], the above simulation of an operation from CLODCC by means of LOCC is an explicit proof of this inclusion. Local operations of enlarging system $\hookrightarrow |0\rangle\langle 0|$, partial trace, and von Neumann projection are explicitly inside LOCC. The operation of application of the shift $S_{i,|s|}$ is controlled by the outcome of the projective measurement on the other system, which employs the communication based interdependencies of the Kraus operators of an LOCC operation.

From the above we have an immediate Corollary, where by $G(\rho_{AB})$ we denote $\log_2 |AB| - S(AB)_\rho$.

Corollary 2. For any two bipartite states ρ and $\tilde{\rho}$ that have positive partial transposition, there is

$$\mathcal{R}_A^{A \leftrightarrow C_1C_2 \leftrightarrow B}(\rho_{AC_1} \otimes \tilde{\rho}_{C_2B}) \leqslant G\big(\rho_{AC_1}^\Gamma \otimes \tilde{\rho}_{C_2B}^\Gamma\big). \quad (36)$$

Proof. We first note that CLODCC($A : C_1C_2 : B$) $\subset$ CLODCC[$A : (C_1C_2B)$] (see Observation 1). The state $\sigma = \rho_{AC_1}^\Gamma \otimes \rho_{C_2B}^\Gamma$, treated as a bipartite state with a partition $A : (C_2C_1B)$, has a positive partial transposition, since ρ_{AC_1} has it positive by assumption. Hence Theorem 1 implies that $G(\sigma)$ is achieved. ■

Since $G(\rho \otimes \tilde{\rho})$ is additive on the tensor product, the RHS of (2) is equal to the RHS of the bound (31) of Corollary 1. So, the above bound is no better than the already presented one. This is in contrast with the case of private key [7], where the corresponding bound was better by a factor of 2 (cf. Lemma 12 and Theorem 13 of the Supplemental Material of [7]).

VI. LIMITATION FOR I.I.D. PRIVATE RANDOMNESS REPEATERS FOR SOME IBITS

In this section we focus on a simpler case in which the three parties first perform the same CLODCC operation on each of the copies of the state, and then A and B perform general CLODCC($A : B$). We begin with defining the rate of repeated private randomness gained by CLODCC[$C^{\mathrm{iid}} : (A^{\mathrm{iid}} : B^{\mathrm{iid}})$] operations. As we will see, in this case even some states with negative partial transposition will have limited repeated private randomness.

We begin with a formal definition of private randomness repeater based on the operations mentioned above:

$$\begin{aligned} &\mathcal{R}_A^{C^{\mathrm{iid}}:(A^{\mathrm{iid}}:B^{\mathrm{iid}})}(\rho_{AC_1} \otimes \tilde{\rho}_{C_2B}) \\ &:= \inf_{\epsilon > 0} \limsup_{n \to \infty} \sup_{\Lambda_n \in \mathrm{CLODCC}[C^{\mathrm{iid}}:(A^{\mathrm{iid}}:B^{\mathrm{iid}})], \alpha_m} \\ &\quad \times \left\{ \frac{m}{n} : \mathrm{Tr}_C \Lambda_n ((\rho_{AC_1} \otimes \tilde{\rho}_{C_2B})^{\otimes n}) \approx_\epsilon \alpha_m \right\} \end{aligned} \quad (37)$$

will be called the quantum i.i.d. private randomness repeater rate of ρ and $\tilde{\rho}$ with respect to CLODCC[$C^{\mathrm{iid}} : (A^{\mathrm{iid}} : B^{\mathrm{iid}})$] operations among A, B, and C, that can be obtained at system A. With a little abuse of notation we will denote $\mathcal{R}_{C^{\mathrm{iid}}:(A^{\mathrm{iid}}:B^{\mathrm{iid}})}$ as $\mathcal{R}_A^{\mathrm{iid}}$. Moreover, in the case of $\rho = \tilde{\rho}$, we will refer to $\mathcal{R}_A^{\mathrm{iid}}(\rho \otimes \tilde{\rho})$ as to $\mathcal{R}_A^{\mathrm{iid}}(\rho)$.

From Lemma 1 of the content of the Supplemental Note 2 in [7], we know the following.

Corollary 3. For any two states ρ_{AC_1} and $\tilde{\rho}_{C_2B}$ and any $\Lambda \in$ CLODCC($A : C_1C_2 : B$), the output state $\hat{\rho}_{AB} = \mathrm{Tr}_C \Lambda(\rho_{AC_1} \otimes \rho_{C_2B})$, satisfies

$$\left\| \hat{\rho}_{AB} - \frac{\mathbb{I}}{|AB|_{\hat{\rho}}} \right\|_1 \leqslant \left\| \rho_{AC_1}^\Gamma - \frac{\mathbb{I}}{|AC_1|} \right\|_1 + \left\| \tilde{\rho}_{C_2B}^\Gamma - \frac{\mathbb{I}}{|C_2B|} \right\|_1. \quad (38)$$

Proof. Follows from $\frac{\mathbb{I}}{d} \in SEP$ and CLODCC $\subset$ LOCC, as a special case of Lemma 1 in [7]. ∎

Proposition 2. For a state $\rho \in \mathbb{C}^d \otimes \mathbb{C}^d$, satisfying $||\rho^\Gamma - \frac{\mathbb{I}}{d}||_1 \leqslant \frac{1}{\mathrm{e}}$, and any operation $\Lambda \in \mathrm{CLODCC}(A : C_1C_2 : B)$, the output state $\hat{\rho}_{AB} = \mathrm{Tr}_C \Lambda(\rho \otimes \rho)$ satisfies

$$\begin{aligned} &|\log_2 |AB|_{\hat{\rho}} - S(AB)_{\hat{\rho}}| \\ &\quad \leqslant 2\left\|\rho^\Gamma - \frac{\mathbb{I}}{d}\right\|_1 \log_2 d + \eta\left(2\left\|\rho^\Gamma - \frac{\mathbb{I}}{d}\right\|_1\right), \end{aligned} \tag{39}$$

where $\eta(x) := -x \log_2 x$.

Proof. From the asymptotic continuity of quantum mutual information [24,25] for any $\rho, \rho' \in \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$ such that $||\rho - \rho'||_1 \leqslant \epsilon$ with $0 < \epsilon < \frac{1}{\mathrm{e}} \approx 0.368$, one has

$$|S(AB)_\rho - S(AB)_{\rho'}| \leqslant \epsilon \log_2 d_{AB} + \eta(\epsilon). \tag{40}$$

Since the von Neumann entropy of the maximally mixed state equals $\log_2 |AB|$, the assertion follows directly from Corollary 3. ∎

We will exemplify the upper bound (39) using the independent state from (12). This state has negative partial transposition. We will use the property

$$\left\|\alpha_{V,d}^\Gamma - \frac{\mathbb{I}}{2d^2}\right\|_1 \leqslant \frac{2}{d}. \tag{41}$$

We are ready to show the gap between private randomness and repeated private randomness for $\alpha_{V,d}$, for sufficiently large d.

Theorem 5. The family of states $\{\alpha_{V,d}\}_{d=2}^\infty$ satisfies the following properties.

(1) For $d > 2$, $R_A(\alpha_{V,d}) = R_B(\alpha_{V,d}) = 1$.

(2) For $d > 11$,

$$\mathcal{R}_A^{\mathrm{iid}}(\alpha_{V,d}) \leqslant \frac{4\log_2 d}{d} + \eta\left(\frac{4}{d}\right). \tag{42}$$

(3) For $d > 32$, $1 = R_A(\alpha_{V,d}) = R_B(\alpha_{V,d}) > \mathcal{R}_A^{\mathrm{iid}}(\alpha_{V,d}) \to_{d\to\infty} 0$.

Proof. The first statement follows from negativity of coherent information of $\alpha_{V,d}$ for $d > 2$, so that Theorem 1 applies. Let us denote $\alpha_{V,d}$ as $\alpha_{AA'B'}$ to indicate subsystems explicitly. Like for the states with positive partial transposition, the conditional entropy $S(B'|AA')$ is equal to the *global purity* of $\alpha_{AA'B'}$, i.e., to $\log_2 |AA'B'| - S(AA'B')_{\alpha_{V,d}}$. This in turn gives $I(AA' : B')_{\alpha_{V,d}} = 1$.

For the second statement, we focus on a perspective of party A. This property follows from the sequence of inequalities:

$$\begin{aligned} \mathcal{R}_A^{\mathrm{iid}}(\alpha \otimes \alpha) &\leqslant R_A(\hat{\rho}) \leqslant \log_2 |AB|_{\hat{\rho}} - S(AB)_{\hat{\rho}} \\ &\leqslant 2\left\|\rho^\Gamma - \frac{\mathbb{I}}{d}\right\|_1 \log_2 d + \eta\left(2\left\|\rho^\Gamma - \frac{\mathbb{I}}{d}\right\|_1\right) \\ &\leqslant \frac{4\log_2 d}{d} + \eta\left(\frac{4}{d}\right), \end{aligned} \tag{43}$$

where $\hat{\rho} = \mathrm{Tr}_C \Lambda(\alpha_{AC_1} \otimes \alpha_{C_2B})$ with $\Lambda \in \mathrm{CLODCC}(A : C_1C_2 : B)$. The first inequality comes from the definition of the class of operations involved in $\mathcal{R}_A^{\mathrm{iid}}$. The second one holds because private randomness cannot be greater than the global purity, i.e., the amount of purity that A and B can obtain when they join their systems and act globally. The value of global purity is achievable due to the Schumacher compression [26,27]. The next inequality follows from Corollary 3. The last one is due to Eq. (41) and the fact that, for $d > 11$, we have $2 \times \frac{2}{d} \leqslant \frac{1}{\mathrm{e}}$ and the Proposition 2. For $d > 32$, the RHS of the just proven bound is less than 1, i.e., less than $R_A(\alpha_{V,d})$. The argument for R_B is symmetric. ∎

The inequality presented in the third item of Theorem 5 seems to be trivial, as R_A involves in its definition a class of operations not restricted by "i.i.d." However, we can make sure that this is not the case for the states $\alpha_{V,d}$ on systems AA'. Indeed, for these states, private randomness is directly accessible for Alice via identical measurements on each copy of $\alpha_{V,d}$ on subsystem A. One can then define R_A^{iid} as private randomness localizable at subsystem of party A via identical operations on the input state.

Corollary 4. For system A of the state $\alpha_{V,d}$ with $d > 32$, there is

$$\mathcal{R}_A^{\mathrm{iid}}(\alpha_{V,d}) < R_A^{\mathrm{iid}}(\alpha_{V,d}). \tag{44}$$

VII. GAP BETWEEN LOCALIZABLE AND REPEATED PRIVATE RANDOMNESS FOR SEPARABLE WERNER STATES

In this section we show that the main result holds for a larger set of Werner states than the fully symmetric state and we briefly study the critical dimension for which there is a limitation in the randomness repeaters.

A general Werner state ρ is a convex combination

$$\rho = (1-\theta)\rho_s + \theta\rho_a, \tag{45}$$

with θ the mixing parameter, the symmetric state $\rho_s := \frac{1}{d^2+d}(\mathbb{I} + V)$, and the antisymmetric state $\rho_a := \frac{1}{d^2-d}(\mathbb{I} - V)$, where V is the swap operator, while d is the dimension of the systems A and B. We will be using the facts that the partial transpose $(\cdot)^\Gamma$ is a linear operator, $(\mathbb{I})^\Gamma = \mathbb{I}$, and $(V)^\Gamma = d|\Phi^+\rangle\langle\Phi^+|$. Using the above results, we write the partial transposes of ρ_s and ρ_a as $(\rho_s)^\Gamma = \frac{\mathbb{I}-|\Phi^+\rangle\langle\Phi^+|}{d^2+d} + \frac{|\Phi^+\rangle\langle\Phi^+|}{d}$ and $(\rho_a)^\Gamma = \frac{\mathbb{I}-|\Phi^+\rangle\langle\Phi^+|}{d^2-d} - \frac{|\Phi^+\rangle\langle\Phi^+|}{d}$. Defining $|\Phi^+\rangle\langle\Phi^+|^\perp := \mathbb{I} - |\Phi^+\rangle\langle\Phi^+|$, we get $\rho^\Gamma = (1-2\theta)\frac{|\Phi^+\rangle\langle\Phi^+|}{d} + [\frac{\theta}{d^2-d} + \frac{1-\theta}{d^2+d}]|\Phi^+\rangle\langle\Phi^+|^\perp$.. The state ρ^Γ is diagonal in the basis of maximally entangled states, called a *Bell basis* [28] because it is a convex combination of Bell diagonal states ρ_s^Γ and ρ_a^Γ. From the form of ρ^Γ one can directly obtain the eigenvalues of ρ^Γ in the Bell basis:

$$\begin{aligned} \lambda_0 &= \frac{(1-2\theta)}{d}, \\ \lambda_1 = \cdots = \lambda_{d^2-1} &= \frac{1}{d}\left[\frac{\theta}{d-1} + \frac{1-\theta}{d+1}\right]. \end{aligned} \tag{46}$$

The eigenvalue λ_0 is associated with the eigenvector $|\Phi^+\rangle$, while all other $d^2 - 1$ eigenvalues are equal and given by (46). Because ρ^Γ is Bell diagonal, the reduction to individual systems A and B gives the maximally mixed state; hence $S(A)_{\rho^\Gamma} = S(B)_{\rho^\Gamma} = \log_2 d$. Computing the entropy of the whole state, which is $S(AB)_{\rho^\Gamma} = \frac{\alpha}{d}\log_2[\frac{1}{\alpha}(\frac{d-\alpha}{d^2-1})] - \log_2[\frac{d-\alpha}{d^2-1}] + \log_2 d$, where $\alpha \equiv 1 - 2\theta$, we are in the

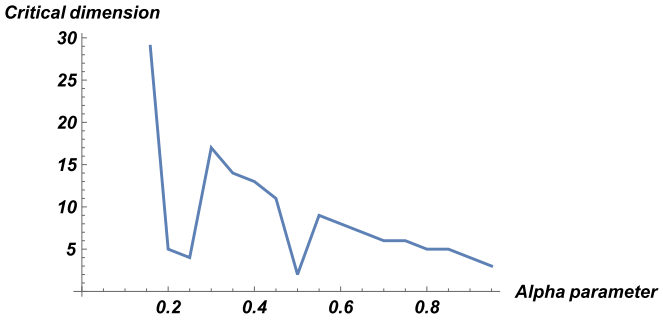

FIG. 4. Values of d_{cri} as the parameter α increases from 0.1 by steps of 0.05. It is worth mentioning some special values, such as $\alpha = 0.1$, for which the d_{cri} takes a very large value of 51, and $\alpha \in \{0.2, 0.5\}$ that determine sudden drops of d_{cri} to the values $\{5, 2\}$, respectively.

position to compute the mutual information:

$$I(A:B)_{\rho^\Gamma} = \log_2\left[\frac{d(d-\alpha)}{d^2-1}\right] + \frac{\alpha}{d}\log_2\left[\frac{\alpha(d^2-1)}{d-\alpha}\right].$$

In consequence,

$$\lim_{d\to+\infty} I(A:B)_{\rho^\Gamma} = 0. \tag{47}$$

As noticed in Sec. I A, the states illustrating our claim are those which satisfy

$$I(A:B)_\rho > 2I(A:B)_{\rho^\Gamma}. \tag{48}$$

Let us notice that states ρ_s and ρ_a have supports, respectively, in the orthonormal subspaces $\mathcal{H}_s$ and $\mathcal{H}_a$ of the full Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_s \oplus \mathcal{H}_a$. The von Neumann entropy of the density matrix $\rho = (\frac{1+\alpha}{2})\rho_s + (\frac{1-\alpha}{2})\rho_a$ reads [see Eq. (12.19) in [29]]

$$\begin{aligned} S(AB)_\rho &= h\left(\frac{1-\alpha}{2}\right) + \frac{1+\alpha}{2}S(AB)_{\rho_s} + \frac{1-\alpha}{2}S(AB)_{\rho_a} \\ &= h\left(\frac{1-\alpha}{2}\right) + \frac{1+\alpha}{2}\log_2(d_+) + \frac{1-\alpha}{2}\log_2(d_-), \end{aligned} \tag{49}$$

where $d_+ = d(d+1)/2$ and $d_- = d(d-1)/2$. Hence the mutual information of the Werner state ρ in the form (45) is

$$I(A:B)_\rho = \log_2\left[\frac{2d}{(d-1)^{(\frac{1-\alpha}{2})}(d+1)^{(\frac{1+\alpha}{2})}}\right] - h\left(\frac{1-\alpha}{2}\right). \tag{50}$$

Hence $\lim_{d\to+\infty} I(A:B)_\rho = 1 - h(\frac{1-\alpha}{2})$. This shows that there always exists a value of d large enough to satisfy the condition (48). The minimum value of d for which the Werner state ρ satisfies (48) will be called the critical dimension d_{cri}.

To understand better the nonlinear dependence of d_{cri}, we also investigate the plot of $I(A:B)_\rho$ and $2I(A:B)_{\rho^\Gamma}$ versus dimension for some selected values of α, as shown in Fig. 4 . The inspection of the sequence presented in Fig. 4 shows that the parameter α essentially induces compression of both curves towards the y axis, which generates the different crossing of the curves as α approaches 1. For the values α greater than 0.5 the value of d_{cri} goes down smoothly and without sudden drops and rises. (See also Fig. 5.)

VIII. TOWARDS TWO-QUBIT EXAMPLES

So far the exemplary states were of dimension higher than $2 \otimes 2$. In this section we show that a wide class of a well known family of states, that of Bell diagonal states (after partial transposition), escapes our technique.

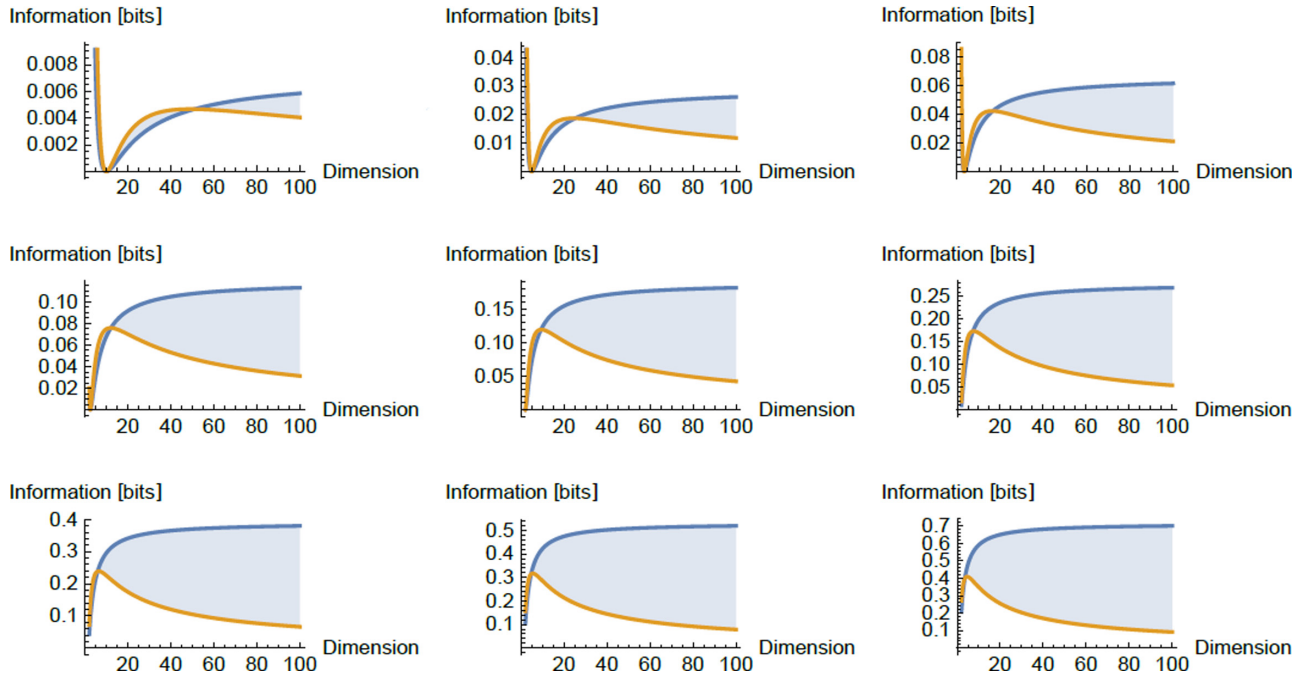

FIG. 5. Plots of information vs dimension show the values of $I(A:B)_\rho$ (blue line) and $2I(A:B)_{\rho^\Gamma}$ (orange line) for several values of α, starting with $\alpha = 0.1$ in the upper left corner and increasing by steps of 0.1 until $\alpha = 0.9$ in the bottom right corner. The solid area highlights the gap between $I(A:B)_\rho$ and $2I(A:B)_{\rho^\Gamma}$.

Any Bell diagonal state can be expressed in the form of a matrix

$$\rho_{\text{Bell}} = \frac{1}{2}\begin{bmatrix} a_+ + a_- & 0 & 0 & a_+ - a_- \\ 0 & b_+ + b_- & b_+ - b_- & 0 \\ 0 & b_+ - b_- & b_+ + b_- & 0 \\ a_+ - a_- & 0 & 0 & a_+ + a_- \end{bmatrix}, \tag{51}$$

where the entries are weights of appropriate Bell states: $\rho_{\text{Bell}} = a_+|\psi_+\rangle\langle\psi_+| + a_-|\psi_-\rangle\langle\psi_-| + b_+|\phi_+\rangle\langle\phi_+| + b_-|\phi_-\rangle\langle\phi_-|$. After partial transposition we obtain the desired family of states:

$$\rho^{\Gamma}_{\text{Bell}} = \frac{1}{2}\begin{bmatrix} a_+ + a_- & 0 & 0 & b_+ - b_- \\ 0 & b_+ + b_- & a_+ - a_- & 0 \\ 0 & a_+ - a_- & b_+ + b_- & 0 \\ b_+ - b_- & 0 & 0 & a_+ + a_- \end{bmatrix}. \tag{52}$$

Since Γ is an involution, we have $(\rho^{\Gamma}_{\text{Bell}})^{\Gamma} = \rho_{\text{Bell}}$. We check now if some of the states of the form $\rho^{\Gamma}_{\text{Bell}} \equiv \rho_{\text{BellG}}$ exhibit a gap between localizable and repeated randomness. Note that every Bell diagonal state has maximally mixed subsystems. Since partial transposition does not change the entropy of the subsystems, the same holds for ρ_{BellG}. Hence the condition $I(A:B)_{\rho_{\text{BellG}}} > 2I(A:B)_{\rho^{\Gamma}_{\text{BellG}}}$ is equivalent to: $S(AB)_{\rho_{\text{BellG}}} < 2S(\rho^{\Gamma}_{\text{BellG}}) - 2$, i.e.,

$$S(AB)_{\rho_{\text{BellG}}} < 2S(AB)_{\rho_{\text{Bell}}} - 2. \tag{53}$$

This condition is equivalent to the following one:

$$\begin{aligned} &2H(\{a_+, a_-, b_+, b_-\}) - 2 \\ &> H\Big(\Big\{\tfrac{1}{2}(a_+ + a_- + b_+ - b_-), \tfrac{1}{2}(a_+ + a_- - b_+ + b_-), \\ &\quad \tfrac{1}{2}(a_+ - a_- + b_+ + b_-), \tfrac{1}{2}(-a_+ + a_- + b_+ + b_-)\Big\}\Big). \end{aligned} \tag{54}$$

We can use the above condition if the state ρ_{Bell} is separable, that is, for $a_+, a_-, b_+, b_- \leqslant \frac{1}{2}$. We have searched for the gap via 5×10^5 random tests of ρ_{Bell} states, yet did not find any case with a gap in Eq. (53). Indeed, for a large region of parameters we are able to confirm that considered states escape our technique.

To see this, let us denote $a_+ = \frac{\alpha_1}{2}$, $a_- = \frac{\alpha_2}{2}$, $b_+ = \frac{\alpha_3}{2}$, and $b_- = \frac{\alpha_4}{2}$. Then the condition of Eq. (54) reads

$$2H\left(\left\{\frac{\alpha_i}{2}\right\}_{i=1}^{4}\right) - 2 > H\left(\left\{\frac{(1-\alpha_i)}{2}\right\}_{i=1}^{4}\right). \tag{55}$$

It turns out that the converse inequality holds, if only $\alpha_i \notin [1/3, 1/2]$ for all $i = 1, \ldots, 4$. This can be seen from expanding $2 = \sum_i \alpha_i$, and observing that the converse inequality holds elementwise:

$$2\eta\left(\frac{\alpha_i}{2}\right) - \alpha_i \leqslant \eta\left(\frac{1-\alpha_i}{2}\right), \tag{56}$$

under considered condition on α_i, where $\eta(x) = -x\log_2 x$. The latter fact is confirmed by plotting the difference of the LHS and RHS using Mathematica 7.0. In terms of parameters $a_\pm$ and $b_\pm$ of the state ρ_{BellG} we cannot decide based on the aforementioned results if the state has limited repeated randomness if $a_\pm, b_\pm \in [0, \frac{1}{6}) \cup (\frac{1}{4}, \frac{1}{2}]$. This fact allows us to conjecture that all the states ρ_{BellG} escape our technique.

IX. DISCUSSION

In this manuscript we have studied the relationship between private key and private randomness obtainable from quantum states, treated as quantum resources. We have shown that the states containing ideal privacy (private dits) belong to the set of states containing ideal private randomness (independent dits). We have then asked if the topology of loyalty in the network of repeaters can be modified by free operations of the resource theory of private randomness. We focused on the simplest repeater: two stations A and B linked by connections with an intermediate station C. The problem we focused on is whether there exists such an action of the three parties that, after performing it, A can relay solely on loyalty of B instead of trusting an intermediate party C. While entanglement swapping is an example of such type of an action in the case of pure (maximally entangled) states, we show that in the case of the mixed states it is not so (in general).

To achieve our goal, in analogy to the rate of the repeated private key, we have defined the rate of repeated private randomness and shown an upper bound on the latter quantity. It is equal to twice the relative entropy with respect to the maximally mixed state. The bound holds for states with positive partial transposition. To exemplify the phenomenon, we showed that the separable Werner states for sufficiently large dimensions exhibit a gap between localizable private randomness and a repeated one. Interestingly, the states used in [7], exhibiting limitation on the repeated key, cannot serve as good examples in our context. This is due to the factor 2 appearing in our upper bound [one cannot achieve the gap between $I(A:B)_\rho$ and $2I(A:B)_{\rho^\Gamma}$]. Improving the bound to characterize the subset of states (especially the subset of separable ones) that exhibit the gap between private and repeated private randomness is an important direction to study. Our Theorem 4 and Corollary 2 are analogs of Lemma 12 and Theorem 13 of [7], respectively. The former yield the same bound as the one presented in our main result (Corollary 1). This is in contrast with the results for the private key. Indeed, in the latter case, the mentioned Theorem 13 of [7] presents the bound on the repeated private key *without* factor 2. However, a study in this direction allowed us to show that for PPT states the repeated private randomness of $\rho \otimes \tilde{\rho}$ is upper bounded by the same function evaluated on $\rho^\Gamma \otimes \tilde{\rho}^\Gamma$, which is of independent interest.

We also studied a limited repeater of private randomness in which the three parties first perform identical operations on each copy, and later perform the best CLODCC protocol on all obtained copies of A and B, without the help of C. We showed that a certain idit, which is not in the PPT set, exhibits an extreme gap for large d. Our findings in this respect do not have a direct analog in [7] and can be extended to hold for a private key.

Presented results open an interesting perspective for further research. First of all one could discuss the implication of results presented in the paper for the simplest possible case, i.e., $2 \otimes 2$ states. The first step toward solution has been made in Sec. VIII, showing that such construction is not straightforward and more sophisticated techniques or candidates are needed.

Secondly, as it was proposed also in [13], one could consider in the context of our paper the amortized approach in which the allowed operations can bring k bits of private randomness (e.g., in the form of purity). The output randomness gets further lowered by k in the end. This is to compute the private randomness content of a given quantum state rather than private randomness of an operation. Since the latter class of operation is still to be explored, we have followed here the approach of [13] based on CLODCC operations.

From the broader perspective we could ask a question: which quantum resources (or just properties of quantum states) are "transferable" via a quantum network of mixed states? We have shown that the limitation on the transfer of certain resources is not bound to private key only. Designing axioms for a resource theory to have limited transfer is an interesting direction of studies.

It is also essential to show an analog of the obtained results for channels rather than states, in the spirit of [30], and for states with negative partial transposition, adopting methods of [31]. Further investigation of interdependencies between private randomness and private key can also lead to fruitful results.

ACKNOWLEDGMENTS

K.H. thanks P. Horodecki for discussion on possible axiomatic approach to presented results, D. Yang for proofreading of an early draft of this manuscript, and A. Winter for sharing an observation that a singlet is an ibit. K.H., R.P.K., and R.S. are supported by the grant Sonata Bis 5 (Grant No. 2015/18/E/ST2/00327) from the National Science Center. K.H. acknowledges partial support by the Foundation for Polish Science through IRAP project co-financed by EU within the Smart Growth Operational Programme (Contract No. 2018/MAB/5).

[1] W. Kozlowski and S. Wehner, in *Proceedings of the Sixth Annual ACM International Conference on Nanoscale Computing and Communication - NANOCOM 19* (ACM Press, New York, 2019).
[2] M. Żukowski, A. Zeilinger, M. A Horne, and A. K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993).
[3] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
[4] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).
[5] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, Phys. Rev. A **59**, 169 (1999).
[6] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).
[7] S. Bäuml, M. Christandl, K. Horodecki, and A. Winter, Nat. Commun. **6**, 6908 (2015).
[8] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. **94**, 160502 (2005).
[9] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, IEEE Trans. Inf. Theory **55**, 1898 (2009).
[10] M. Bera, A. Acín, M. Kuś, M. Mitchell, and M. Lewenstein, Rep. Prog. Phys. **80**, 124001 (2017).
[11] M. Berta, O. Fawzi, and S. Wehner, IEEE Trans. Inf. Theory **60**, 1168 (2014).
[12] https://www.idquantique.com/.
[13] D. Yang, K. Horodecki, and A. Winter, Phys. Rev. Lett. **123**, 170501 (2019).
[14] E. Chitambar and G. Gour, Rev. Mod. Phys. **91**, 025001 (2019).
[15] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer, Dordrecht, 1993).
[16] M. Horodecki, P. Horodecki, R. Horodecki, J. Oppenheim, A. Sen(De), U. Sen, and B. Synak-Radtke, Phys. Rev. A **71**, 062307 (2005).
[17] K. Horodecki, Ł. Pankowski, M. Horodecki, and P. Horodecki, IEEE Trans. Inf. Theory **54**, 2621 (2008).
[18] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
[19] J. Oppenheim, M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **89**, 180402 (2002).
[20] A. Streltsov, G. Adesso, and M. B. Plenio, Rev. Mod. Phys. **89**, 041003 (2017).
[21] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).
[22] K. Horodecki, D. Leung, H.-K. Lo, and J. Oppenheim, Phys. Rev. Lett. **96**, 070501 (2006).
[23] M. Piani, Phys. Rev. Lett. **103**, 160504 (2009).
[24] R. Alicki and M. Fannes, J. Phys. A: Math. Gen. **37**, L55 (2004).
[25] M. Shirokov, J. Math. Phys. **58**, 102202 (2017).
[26] B. Schumacher, Phys. Rev. A **51**, 2738 (1995).
[27] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2000).
[28] R. Werner, J. Phys. A: Math. Gen. **34**, 7081 (2001).
[29] I. Bengtsson and K. Życzkowski, *Geometry of Quantum States. An Introduction to Quantum Entanglement* (Cambridge University Press, Cambridge, UK, 2006).
[30] M. Christandl and A. Müller-Hermes, Commun. Math. Phys. **353**, 821 (2017).
[31] M. Christandl and R. Ferrara, Phys. Rev. Lett. **119**, 220506 (2017).