Min-entropy as a resource for one-shot private state transfer, quantum masking, and state transition

Seok Hyung Lie, Seongjeon Choi, and Hyunseok Jeong*
Department of Physics and Astronomy, Seoul National University, Seoul 151-742, Korea

(Received 6 November 2020; accepted 24 March 2021; published 23 April 2021)

We give an operational meaning to the min-entropy of a quantum state as a resource measure for various interconnected tasks. In particular, we show that the min-entropy without smoothing measures the amount of quantum information that can be hidden or encoded perfectly in the one-shot setting when the quantum state is used as a randomness or correlation source. First, we show that the min-entropy of entanglement of a pure bipartite state is the maximum number of qubits privately transferable when the state is used as a quantum one-time pad. Then, through the equivalence of quantum secret sharing–like protocols, it is also shown that the min-entropy of a quantum state is the maximum number of qubits that can be masked when the state is used as a randomness source for a quantum masking process. Consequently, we show that the min-entropy of a quantum state is half the size of the quantum state it can catalytically dephase. This gives a necessary and sufficient condition for catalysts for state transition processes.

DOI: 10.1103/PhysRevA.103.042421

I. INTRODUCTION

The space of quantum correlation is vast. The dimension of a collection of many quantum systems is much larger than the sum of the dimension of each system. This concept has motivated research on the method of encoding information within a global quantum state without altering local quantum systems. Such efforts have appeared under many names: quantum error correcting codes [1,2], quantum secret sharing [3,4], quantum masking [5–7], and private state transfer [8,9].

Among these tasks, quantum secret sharing (QSS) [4] is especially important since, as we will see, it subsumes many other similar tasks. Quantum secret sharing is the task of distributing an arbitrary quantum state to multiple parties in a fashion by which only authorized subsets of them can restore the quantum state. Each local party's marginal state (share) of a QSS scheme should have a constant form regardless of the quantum secret. Typically each share of a QSS scheme is a quantum state that should be stored in a quantum system. However, it is still demanding to maintain a large quantum system protected from noise and error. Thus, estimating and optimizing the informational size of the each share is critical, since it is directly related to the required physical size of the storage medium to contain each share.

The informational size of a quantum system is decided by how random the system is. There have been studies on lower bounds of the amount of randomness of each share in a QSS scheme. The Rényi entropy [10], defined as

$$S_\alpha(\rho) \equiv \frac{1}{1-\alpha}\log_2 \mathrm{Tr}[\rho^\alpha], \tag{1}$$

and its limits, i.e., the max-entropy $S_{\max}(\rho) \equiv \log_2 \mathrm{rank}(\rho) = \lim_{\alpha\to 0} S_\alpha(\rho)$, the min-entropy $S_{\min}(\rho) \equiv -\log_2 \|\rho\| = \lim_{\alpha\to\infty} S_\alpha(\rho)$ (here $\|\rho\|$ is the operator norm of ρ which is the largest singular value of ρ), and the von Neumann entropy $S(\rho) \equiv -\mathrm{Tr}[\rho\log_2\rho] = \lim_{\alpha\to 1} S_\alpha(\rho)$ [11], are often used to quantify the randomness within a quantum state ρ. In Ref. [3] it was proven that, for an arbitrary secret sharing scheme for a d-dimensional quantum secret, the dimension of each share of secret must be at least as large as the dimension of the secret itself. This provides a lower bound for the max-entropy of each share denoted by σ, i.e., $S_{\max}(\sigma) \geqslant \log_2 d$. In Refs. [12,13] the result was improved to provide a lower bound of the von Neumann entropy of each share, i.e., $S(\sigma) \geqslant \log_2 d$. Note that the Rényi entropy monotonically decreases as α grows [14].

The problem, however, was not closed, since the optimality of the lower bound was not proved. Can any quantum state with the von Neumann entanglement entropy larger than $\log_2 d$ be a marginal state of a QSS scheme? If not, when is it possible?

In this work we show that these questions are intimately related to other questions about the amount of required resources for many other important quantum information processing tasks. We then close this problem by giving the min-entropy of a quantum state operational meanings as the power for tasks such as private state transfer, quantum masking, and implementation of a dephasing map.

For example, for the quantum masking [5,13,15], the task of hiding quantum information in a bipartite quantum correlation using a randomness source and bipartite interaction, the amount quantum information that can be masked by a randomness source is given by its min-entropy. For the private state transfer [8], the task of transmitting a quantum state without giving any information to a potential eavesdropper by utilizing preestablished quantum correlation, the amount of privately transferable quantum information is determined by the min-entropy of the marginal state of the preestablished pure bipartite state. In doing so, we introduce a deterministic method of randomness extraction from a weak quantum randomness source, i.e., a mixed state with high enough

*h.jeong37@gmail.com

min-entropy but having nonuniform eigenvalues, utilizing the Nielsen theorem [16].

These results imply an important consequence for state transition processes under the constraint that randomness is not free, which is deeply related to quantum thermodynamics [17,18]. We completely characterize the randomness sources that can dephase a given size of quantum system. As a direct consequence, we derive a necessary and sufficient criterion for the possibility of a state transition process with a given catalyst [19].

Our paper is organized as follows. In Sec. II the definitions of QSS-like tasks, private state transfer, and quantum masking are given and their equivalence is shown. Readers who are not familiar with QSS schemes could refer to this section. In Sec. III we prove that the minimal min-entropy of entanglement of a one-time pad for privately transferring a d-dimensional quantum state is $\log_2 d$. In Sec. IV, through the equivalence with private state transfer established in Sec. II, we prove that the minimal min-entropy of a randomness source for masking a d-dimensional quantum state is also $\log_2 d$. In Sec. V we introduce dephasing processes with leftover randomness and show that $\log_2 d$ bits of randomness are required for a catalytic transition between two d^2-dimensional quantum states in a majorization relation. In Sec. VI we summarize the results of our paper and discuss possible future work.

II. EQUIVALENCE OF QSS-LIKE TASKS

A QSS scheme is a quantum process that encodes a quantum state into a multipartite state such that only authorized subsets of the participants can restore the encoded state. An important type of QSS scheme is the $((k,n))$-threshold QSS scheme, which is a process that encodes an arbitrary quantum state into an n-partite quantum state such that only subset of n parties with size larger than $k-1$ can restore the encoded secret quantum state.

We will denote the Hilbert space corresponding to quantum system A by $\mathcal{H}_A$ and the vector space of operators on the Hilbert space $\mathcal{H}_A$ by $\mathcal{B}(\mathcal{H}_A)$. We will also follow the convention of denoting the marginal state on system A of a multipartite state $|\Psi\rangle_{ABC\ldots}$ by Ψ_A throughout this work. In the following definition, families of quantum channels defined on $\mathcal{B}(\mathcal{H}_A)$ with the form $\{\mathcal{E}_\psi\}$ will be considered, where the index ψ can be an arbitrary d-dimensional quantum state. Technically, the $((k,n))$-threshold QSS scheme can be defined as follows.

Definition 1 (quantum secret sharing). A $((k,n))$-threshold QSS scheme is a quantum channel $\mathcal{Q}:\mathcal{B}(\mathcal{H})\to\bigotimes_{i\in\mathcal{P}}\mathcal{B}(\mathcal{H}_i)$ with $|\mathcal{P}|=n$ such that for all $\mathcal{F}\subseteq\mathcal{P}$ with $|\mathcal{F}|<k$, $\mathrm{Tr}_{\mathcal{P}\setminus\mathcal{F}}\circ\mathcal{Q}$ is a constant channel and for any $\mathcal{A}\subseteq\mathcal{P}$ with $|\mathcal{A}|\geqslant k$ there exists a quantum channel $\mathcal{R}_\mathcal{A}$ such that $\mathcal{R}_\mathcal{A}\circ\mathrm{Tr}_{\mathcal{P}\setminus\mathcal{A}}\circ\mathcal{Q}(\rho)=\rho$.

It was proven that [3,4] only the schemes with $n/2<k\leqslant n$ are allowed by the no-cloning theorem and that secret sharing through pure n-partite state is possible only for $((k,2k-1))$-threshold QSS schemes. In particular, the impossibility of pure ((2,2))-threshold QSS schemes (named masking quantum information or quantum masking) was recently rediscovered under the name of the no-masking theorem [5]. Subsequently, two approaches to circumvent the no-masking theorem have emerged. One is to keep the pureness of the output state and to restrict the set of quantum states to be "masked" (meaning hidden from two local parties) [7,20]. Another is to give up the pureness while keeping the universality, the property of being able to mask any quantum state, by employing the source of randomness [13,15], which is required for any reversible mixed process by the result of Nayak and Sen [21]. When it is necessary to distinguish them, we will call the former schemes unitary masking processes and the latter randomized masking processes. Note that randomized masking is different from probabilistic masking, which was recently proved to be impossible as well [6]. A randomized masking process is an invertible quantum process and therefore should have a form of isometry by the result of Ref. [21]; we establish it as a technical definition of the randomized masking process.

Definition 2 (quantum masking). A randomized masking process $\mathcal{T}:\mathcal{B}(\mathcal{H}_A)\to\mathcal{B}(\mathcal{H}_A\otimes\mathcal{H}_B)$ is a ((2,2))-threshold QSS scheme with the form for any input state ρ,

$$\mathcal{T}(\rho)=V(\rho\otimes\zeta)V^\dagger, \tag{2}$$

with a unitary operator V on $\mathcal{H}_A\otimes\mathcal{H}_B$ and some mixed state ζ, where both partial traces $\mathrm{Tr}_A\circ\mathcal{T}$ and $\mathrm{Tr}_B\circ\mathcal{T}$ are constant quantum maps.

In other words, Definition 2 requires both $\mathrm{Tr}_A\mathcal{T}(\rho)$ and $\mathrm{Tr}_B\mathcal{T}(\rho)$ to be constant for every input state ρ. Here ζ acts as a source of randomness and will be called the safe state of the masking process [13]. It is called a safe state in the sense that quantum information is securely masked as if it is being stored safely in a virtual safe. The masking process masks quantum information since both local parties cannot access the masked quantum state. Since our focus in this work is on universal processes, when we refer to masking processes without specification, it will be the randomized masking processes.

Next we give the definition of encoding schemes for faithful one-shot private state transfer (PST). Consider a situation in which two parties, Alice and Bob, have a predistributed entangled state $|\Psi\rangle_{AB}$. Alice encodes her possibly unknown quantum state ψ by making ψ interact with her part of $|\Psi\rangle_{AB}$. This results in the secret encoding channel Φ_ψ acting on the system A of $|\Psi\rangle_{AB}$. Then Alice transmits system A to Bob over a quantum channel. However, to make the secret remain private, any possible eavesdropper seizing the transmitted state $\Phi_\psi(\mathrm{Tr}_B|\Psi\rangle\langle\Psi|_{AB})$ should gain no information at all about the state ψ. To finish the transmission, there also should be a recovery map that can recover ψ from $(\Phi_\psi\otimes\mathcal{I})(|\Psi\rangle\langle\Psi|_{AB})$. We will focus on the case where this recovery map exactly recovers the secret state, in contrast to *approximate* recovery. Now we give the technical description of this task.

Definition 3 (private state transfer). A family of quantum channels $\{\Phi_\psi\}$ is said to encode quantum state ψ into a bipartite state $|\Psi\rangle_{AB}$ for d-dimensional faithful one-shot PST if $\Phi_\psi(\Psi_A)$ is constant regardless of ψ and there exists a unitary operator M on $\mathcal{H}_A\otimes\mathcal{H}_B$ such that $\mathrm{Tr}_B(M^\dagger(\Phi_\psi\otimes\mathcal{I}_B)(|\Psi\rangle\langle\Psi|_{AB})M)=\psi$.

We say that $|\Psi\rangle_{AB}$ given above is used as a quantum one-time pad for faithful one-shot private transfer of a d-dimensional quantum state. We will drop the modifiers

"faithful" and "one-shot" in the following unless they are necessary.

By definition, both marginal states of the output bipartite state of a PST process should be independent of the input state. Therefore, every PST process stopped before actual transmission is a ((2,2))-threshold QSS process.

The equivalence of quantum masking and PST is evident from the fact that both are simply two different expressions of general ((2,2))-threshold QSS schemes, but it can also be shown explicitly.

Lemma 1. Private state transfer and quantum masking are equivalent.

Proof. We first note that every extension of a mixed state can be obtained by applying a quantum channel to the purifying system of a purification of the mixed state. For example, let τ_A be a quantum state and τ_{AB} be an extension of it. A purification of an extension is also a purification of the mixed state, which can be verified by applying the partial trace of the former to obtain the original mixed state. It is also known that every purification of a quantum state is unitarily similar when applied on the purifying system. Therefore, for a purification of τ_A, τ_{AE}, and a purification of τ_{AB}, τ_{ABC}, which is also a purification τ_A, there exists a unitary operator $W_{E\to BC}$ such that $W_{E\to BC}\tau_{AE}W_{E\to BC}^\dagger = \tau_{ABC}$. By taking the partial trace, we get $\tau_{AB} = \mathrm{Tr}_C[W_{E\to BC}\tau_{AE}W_{E\to BC}^\dagger]$. Since applying the unitary operator and taking the partial trace is a quantum channel, we obtain the desired result.

We follow the notation and assumptions of Definitions 2 and 3. We can extend a family of quantum channels $\{\Phi_\psi\}$ for an arbitrary operator from linearity, i.e., $\Phi_{a\psi+b\phi} := a\Phi_\psi + b\Phi_\phi$. Then, if $\{\Phi_\psi\}$ is a family of linear maps such that $\mathrm{Tr}_B[M^\dagger(\Phi_\psi \otimes \mathcal{I}_B)(|\Psi\rangle\langle\Psi|_{AB})M] = \psi$ for all ψ, the channel $\mathcal{C}$ defined as $\mathcal{C}(\rho) = \mathrm{Tr}_B[M^\dagger(\Phi_\rho \otimes \mathcal{I}_B)(|\Psi\rangle\langle\Psi|_{AB})M]$ is the identity channel as it preserves every input state. Therefore, for a maximally entangled state $|\Xi\rangle_{RA} = d^{-1/2}\sum_i |ii\rangle_{RA}$, $(\mathcal{I}_R \otimes \mathcal{C})(|\Xi\rangle\langle\Xi|_{RA}) = |\Xi\rangle\langle\Xi|_{RA}$. Since it is a pure state, every purification of this state should be in a product state. Therefore, an extension of $(\mathcal{I}_R \otimes \mathcal{C})(|\Xi\rangle\langle\Xi|_{RA})$, $\frac{1}{d}\sum_{ij}|i\rangle\langle j|_R \otimes M^\dagger(\Phi_{|i\rangle\langle j|} \otimes \mathcal{I}_B)(|\Psi\rangle\langle\Psi|_{AB})M$, can be obtained by applying a quantum channel to the purifying systems uncorrelated with RA. Since an uncorrelated system cannot become correlated after applying a local operation, we get that $\frac{1}{d}\sum_{ij}|i\rangle\langle j|_R \otimes M^\dagger(\Phi_{|i\rangle\langle j|} \otimes \mathcal{I}_B)(|\Psi\rangle\langle\Psi|_{AB})M = |\Xi\rangle\langle\Xi|_{RA} \otimes \zeta$ for some quantum state ζ. By the Choi-Jamiołkowski isomorphism [22,23], we get $M^\dagger(\Phi_\psi \otimes \mathcal{I}_B)(|\Psi\rangle\langle\Psi|_{AB})M = \psi \otimes \zeta$ for an arbitrary quantum state ψ. Therefore, it follows that $(\Phi_\psi \otimes \mathcal{I}_B)(|\Psi\rangle\langle\Psi|_{AB}) = M(\psi \otimes \zeta)M^\dagger$, where both partial traces of the right-hand side are constant quantum maps for ψ by Definition 3. Hence every PST is a quantum masking process.

Conversely, consider a quantum masking process $\mathcal{T}(\rho) = V(\rho \otimes \zeta)V^\dagger$ that has constant marginal state $\Psi_B \equiv \mathrm{Tr}_A\mathcal{T}$. We consider a purification $|\Psi\rangle_{AB}$ of Ψ_B. Since every extension of a mixed state can be made by applying a quantum channel to its purifying system of the state's purification, for every input state ρ there exists a corresponding quantum map Φ_ρ acting on A such that $(\Phi_\rho \otimes \mathcal{I}_B)(|\Psi\rangle\langle\Psi|_{AB}) = \mathcal{T}(\rho)$. It follows that $\mathrm{Tr}_A(\Phi_\rho \otimes \mathcal{I}_B)(|\Psi\rangle\langle\Psi|_{AB}) = \Psi_B$ is a constant state regardless of ρ and that $\mathrm{Tr}_B V^\dagger(\Phi_\rho \otimes \mathcal{I}_B)(|\Psi\rangle\langle\Psi|_{AB})V = \mathrm{Tr}_B(\rho \otimes \zeta) = \rho$. Therefore, $\{\Phi_\rho\}$ is a family of quantum channels that satisfies Definition 3. ∎

Lemma 1 only proves that the input-output relations of PST and quantum masking are equivalent and the two tasks are still different in terms of the physical implementation method. Private state transfer requires a predistributed entangled state, but encoding itself can be executed locally; in contrast, quantum masking requires no entangled state but should be implemented with global interaction of two quantum systems.

The equivalence of the lower bounds of measures for the randomness source of quantum masking and a quantum one-time pad of PST can be explicitly shown in the following way. It is known that any purification of the ((2,2))-threshold QSS scheme is a ((2,3))-threshold QSS scheme [4]. It follows from the no-hiding theorem [24], which states that if a quantum state is completely erased from a system it can be recovered unitarily from its purifying system. From the no-hiding theorem, any two of the three elements, i.e., participants A and B of the ((2,2))-threshold QSS scheme and their purifying environment E, can restore the encoded state since any of A and B has no information at all about the encoded state. The purifying environment E also has no information about the state since it has never interacted with the encoder. This indicates that a purification of the ((2,2))-threshold QSS scheme is a ((2,3))-threshold QSS scheme. Also, by discarding any one share of a ((2,3))-threshold QSS scheme one obtains a ((2,2))-threshold QSS scheme. This follows immediately from the definition of the threshold QSS scheme since discarding grants no additional information to individual participants, but two participants can still collectively restore the encoded state as there are two of them remaining.

A purification of the arbitrary masking process $\mathcal{T}(\rho)$ given in Eq. (2) can be obtained by purifying the safe state ζ, i.e.,

$$(V_{AB} \otimes \mathbb{1}_C)(\rho_A \otimes |Z\rangle\langle Z|_{BC})(V_{AB}^\dagger \otimes \mathbb{1}_C), \tag{3}$$

where $|Z\rangle_{BC}$ is a purification of the mixed state ζ. Since this is a ((2,3))-threshold QSS scheme, by tracing out system A, one gets another ((2,2))-threshold QSS scheme of the form

$$(\Phi_\rho \otimes \mathcal{I}_C)(|Z\rangle\langle Z|_{BC}), \tag{4}$$

with $\Phi_\rho(\sigma) \equiv \mathrm{Tr}_A[V(\rho \otimes \sigma)V^\dagger]$ defined for every quantum state ρ, which exactly fits the definition of PST. One can easily check that a similar argument holds for the converse case. Therefore, the Rényi entanglement entropy of the quantum one-time pad $|Z\rangle$ is the same as the Rényi entropy of the safe state ζ. Thus, by lower bounding the former, one can also lower bound the latter.

III. PRIVATE STATE TRANSFER

In this section, we give a necessary and sufficient condition that a pure bipartite quantum state $|\Psi\rangle_{AB}$ should satisfy in order to be used for PST. For this purpose, we use the result of Nielsen's theorem [16], stated in the following form [25]. Here, that the quantum state ρ majorizes another quantum state σ means that the spectrum of ρ majorizes that of σ, i.e., $\sum_{i=1}^k \lambda_i(\rho) \geqslant \sum_{i=1}^k \lambda_i(\sigma)$ for all k where $\lambda_i(\rho)$ is the ith largest eigenvalue of ρ.

Lemma 2 (Nielsen theorem). For two pure bipartite states $|\Psi\rangle_{AB}$ and $|\Phi\rangle_{AB}$ such that Ψ_A is majorized by Φ_A, there

exists a one-way local operation and classical communication (LOCC) superoperator Λ on $\mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$ given in the form

$$\Lambda(\omega) = \sum_i (K_i \otimes U_i)\omega(K_i^\dagger \otimes U_i^\dagger), \tag{5}$$

where $\{K_i\}$ forms the set of Kraus operators, i.e., $\sum_i K_i^\dagger K_i = \mathbb{1}_A$, and U_i are unitary operators acting on $\mathcal{H}_B$ such that $\Lambda(|\Psi\rangle\langle\Psi|_{AB}) = |\Phi\rangle\langle\Phi|_{AB}$.

Theorem 1. A bipartite state $|\Psi\rangle_{AB}$ can be used as a quantum one-time pad for faithful private transfer of a d-dimensional quantum state if and only if $S_{\min}(\Psi_A) \geqslant \log_2 d$.

Proof. Suppose that $S_{\min}(\Psi_A) \geqslant \log_2 d$. This is equivalent to the spectrum of Ψ_A being majorized by $(1/d, \ldots, 1/d, 0, \ldots)$. If $|\Phi\rangle_{AB}$ is a maximally entangled state on some d-dimensional subspaces of $\mathcal{H}_A$ and $\mathcal{H}_B$, by Nielsen's theorem, there exists a one-way LOCC superoperator Λ on $\mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$ given (5) such that $\Lambda(|\Psi\rangle\langle\Psi|_{AB}) = |\Phi\rangle\langle\Phi|_{AB}$. We modify this superoperator so that the classical communication from Alice to Bob is suspended and stored in a data storage of Alice, i.e., we extend the superoperator Λ to $\tilde{\Lambda} : \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B) \to \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathbb{C}^m)$ for some m (we will refer to the system $\mathbb{C}^m$ as C) given as

$$\tilde{\Lambda}(\omega) = \sum_i (K_i \otimes U_i)\omega(K_i^\dagger \otimes U_i^\dagger) \otimes |i\rangle\langle i| \tag{6}$$

and similarly define $\Xi : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_A \otimes \mathbb{C}^m)$ as

$$\Xi(\omega) = \sum_i K_i \omega K_i^\dagger \otimes |i\rangle\langle i|. \tag{7}$$

Note that $\Lambda(|\Psi\rangle\langle\Psi|_{AB}) = \mathrm{Tr}_C \circ \tilde{\Lambda}(|\Psi\rangle\langle\Psi|_{AB}) = |\Phi\rangle\langle\Phi|_{AB}$ and $|\Phi\rangle\langle\Phi|_{AB}$ is a pure state; therefore, $\tilde{\Lambda}(|\Psi\rangle\langle\Psi|_{AB})$ should have the form of $|\Phi\rangle\langle\Phi|_{AB} \otimes \sigma_C$, with some σ, i.e., other systems should be decoupled from a system in a pure state. Then we can see that $\Xi(\Psi_A) = \Phi_A \otimes \sigma_C$ for some mixed state σ because $\Xi(\Psi_A) = \mathrm{Tr}_B \circ \tilde{\Lambda}(|\Psi\rangle\langle\Psi|_{AB})$.

Since Φ_A is a quantum state with uniform nonzero eigenvalues $1/d$, there exists [13,15] a family of secret encoding maps $\{\Theta_\psi\}$ of d-dimensional quantum states such that $\Theta_\psi(\Phi_A)$ is constant for all ψ. If we let $\{(\Theta_\psi \otimes \mathcal{I}_C) \circ \Xi\}$ be the family of secret encoding maps acting on A of $|\Psi\rangle_{AB}$, we get the wanted result. The secret can be restored by first applying U_i on B conditioned on C followed by discarding the system C and applying the restoring map for $\{\Theta_\psi\}$ on AB. The first step transforms $|\Psi\rangle_{AB}$ to $|\Phi\rangle_{AB}$, which is the legitimate safe-key state [13,15] of $\{\Theta_\psi\}$ so that the second step works.

Conversely, suppose that there exists a family of secret encoding maps $\{\Theta_\psi\}$ of d-dimensional quantum states acting on A of $|\Psi\rangle_{AB}$. It is equivalent to there existing a quantum masking process that uses Ψ_A as the safe state [13]. Therefore, according to Eq. (9) of Ref. [15], every eigenvalue p_i of Ψ_A must not be larger than $1/d$.[1] Since it is equivalent to $S_{\min}(\Psi_A) \geqslant \log_2 d$, the wanted result is obtained. ■

This result generalizes the result of Ref. [26] that if $S_{\min}(\Psi_A) \geqslant \log_2 d$, then $|\Psi\rangle_{AB}$ can be used for faithfully teleporting a d-dimensional quantum state, since the quantum teleportation is a special case of PST. Note that any eavesdropper of the classical communication in a teleportation protocol without sharing initial entanglement cannot gain any information of the teleported quantum state. Also, Theorem 1 shows that the faithful teleportation protocol given in Ref. [26] is not only an optimal teleportation protocol, but also an optimal PST protocol in the sense that the protocol consumes the minimal amount of entangled state without any leftover entanglement and does not require a quantum channel between Alice and Bob for the secret recovery. Nonetheless, note that teleportation is not the only possible PST scheme. From Lemma 1 it follows that any output state of a quantum masking process is also an output state of a PST. However, the output state of a teleportation (as a PST process) is a classical quantum state, but since there are quantum masking processes with entangled outputs [13], it follows that there are nonteleportation PST schemes too.

If we define the one-shot PST power of $|\Psi\rangle_{AB}$ as the maximal size of the transferable quantum state by using state $|\Psi\rangle_{AB}$ counted in qubits as $P_p(|\Psi\rangle_{AB}) \equiv \log_2 \lfloor 2^{S_{\min}(\Psi_A)} \rfloor$, we have the following result.

Corollary 1. The one-shot PST power for bipartite states is superadditive, i.e., $P_p(|\Psi\rangle \otimes |\Phi\rangle) \geqslant P_p(|\Psi\rangle) + P_p(|\Phi\rangle)$.

IV. QUANTUM MASKING

From the equivalence and duality of quantum masking and PST, we can similarly define the masking power of a quantum state σ as $P_m(\sigma) \equiv \lfloor 2^{S_{\min}(\sigma)} \rfloor$. We will say that a quantum state σ can mask d-dimensional quantum information when it is used as the safe state of a d-dimensional randomized quantum masking process. The main result implies the following.

Corollary 2. A quantum state σ can mask d-dimensional quantum information if and only if $S_{\min}(\sigma) \geqslant \log_2 d$. Moreover, the masking power quantum state is superadditive, i.e., $P_m(\sigma_1 \otimes \sigma_2) \geqslant P_m(\sigma_1) + P_m(\sigma_2)$.

Note that, by appropriately merging unauthorized sets of an arbitrary $((k, n))$-threshold QSS scheme, one can construct a ((2,2))-threshold scheme [13,15], i.e., quantum masking. Therefore, Corollary 2 applies to an arbitrary unauthorized set of d-dimensional QSSs; i.e., any unauthorized party's marginal state should have min-entropy larger than or equal to $\log_2 d$.

This result implies that having large von Neumann entropy alone is not enough for masking quantum information. For example, a rank-3 quantum state with the spectrum of (0.7730,0.1135,0.1135) has 1 bit of von Neumann entropy, but since its min-entropy is 0.3716 bits, it cannot mask a qubit of quantum information. On the other hand, a state with the spectrum of $(1/2, 1/4, 1/8, \ldots, 1/2^n, 1/2^n)$ which has 1 bit of min-entropy can mask a qubit of quantum information even though its randomness is highly nonuniform. The consequences of Theorem 1 is not limited to quantum information processing tasks but also has implications for the field of state transition.

V. STATE TRANSITION

For any initial state ρ and final state ρ', implementation of a quantum channel (transition) $\mathcal{E}$ such that $\mathcal{E}(\rho) = \rho'$ by

[1] Since $I(R:A)_{\tau_{RA}} + I(R:B)_{\tau_{RB}} = 2\log d$ and $\max\{I(R:A)_{\tau_{RA}}, I(R:B)_{\tau_{RB}}\} \leqslant -\log p_i$, we get $\log d \leqslant -\log p_i$ for all i.

utilizing randomness has been studied [17,19,27]. Every state transition process can be realized if a dephasing map can be realized [19,27] due to the Schur-Horn theorem [28], since every state transition between two states with a majorization relation can be decomposed into the initial unitary evolution followed by a dephasing map and the final unitary evolution.

Lemma 3 (Schur-Horn theorem). A probability distribution $(p_i) \in \mathbb{R}^n$ majorizes another distribution $(q_i) \in \mathbb{R}^n$ if and only if there exists an $n \times n$ unitary matrix $U = (U_{ij})$ such that $q_i = \sum_j |U_{ij}|^2 p_j$.

Therefore, realizing dephasing maps is the essential part of implementing a state transition. The necessary and sufficient condition for the source of randomness (SOR) of the dephasing channel can also be obtained from Theorem 1. Here we will use a slightly different definition of the (catalytic) dephasing map using quantum randomness to encompass the usage of an imperfect SOR [29]. We will say the map $\mathcal{E}$ dephases with respect to a certain basis $\{|i\rangle\}$ using a SOR σ with a leftover SOR η if there exists an isometry operator (a unitary operator that embeds a smaller Hilbert space into a larger one) U acting on AB such that for any d-dimensional quantum state ρ,

$$\mathcal{E}(\rho) = \mathrm{Tr}_B[U(\rho \otimes \sigma)U^\dagger] = \sum_i \langle i|\rho|i\rangle |i\rangle\langle i| \otimes \eta, \quad (8)$$

and there exists some quantum state τ on B so that the complement channel of $\mathcal{E}$ has the form

$$\tilde{\mathcal{E}}(\rho) = \mathrm{Tr}_A[U(\rho \otimes \sigma)U^\dagger] = \tau, \quad (9)$$

regardless of ρ. We will say the use of a SOR σ is catalytic when τ can also be used for some d-dimensional dephasing map with the same property, i.e., it is an infinitely recyclable SOR. One can see that this definition is recursive. We will also say that σ (catalytically) dephases d-dimensional quantum states for the same situation. The leftover SOR η does not cause problems since it can always be stored or discarded independently of the dephasing process itself, since it is in a product state with the dephased state of the input ρ. If the second requirement is not imposed, then SOR is not needed at all since a simple controlled-NOT gate can dephase with a pure ancillary system. (See Ref. [29] for a more detailed discussion on this generalized setting.)

In Ref. [19], only maximally mixed SORs were considered when the minimal randomness bound was derived and only approximate dephasing was considered for potentially nonuniform SORs, but since it is well known that nonuniform randomness sources can cause security issues [30,31], it is necessary to analyze the power of nonuniform SORs. In the following theorem, we give a necessary and sufficient condition of when a SOR can be used to *exactly* dephase an arbitrary input state.

Theorem 2. A quantum state σ can dephase d^2-dimensional quantum states catalytically if and only if $S_{\min}(\sigma) \geqslant \log_2 d$.

Proof. Suppose that σ can dephase d^2-dimensional quantum states. Then, by using two copies of σ, i.e., $\sigma \otimes \sigma$, one can mask any d^2-dimensional quantum state ρ by dephasing it into two mutually unbiased bases. For example, one can use one σ to dephase ρ and apply the (d^2-dimensional) discrete Fourier transform gate [defined as $\sum_{n,m=1}^{d^2} \exp(i2\pi nm/d^2)|n\rangle\langle m|$] to the output. Then, by using the other σ, one can dephase the output state with respect to the same basis. The final output state is the d^2-dimensional maximally mixed state for every input state ρ (with some leftover SOR in a product state). Since the SOR $\sigma \otimes \sigma$ is also transformed into a quantum state that is independent of ρ, the whole process is a randomized masking process. Therefore, by Corollary 2, $S_{\min}(\sigma \otimes \sigma) \geqslant 2\log_2 d$. By the additivity of the min-entropy, we get $S_{\min}(\sigma) \geqslant \log_2 d$.

Conversely, assume that $S_{\min}(\sigma) \geqslant \log_2 d$. If we pick a purification $|\Sigma\rangle$ of σ, then one can replace $|\Psi\rangle$ in the proof of Theorem 1 with $|\Sigma\rangle$ since it majorizes a d-dimensional maximally entangled state $|\Phi\rangle$. Therefore, we will use the corresponding Kraus operators $\{K_i\}$ defined in the same way as in Eq. (6). Then we apply the isometry operator $\sum_i |i\rangle_{A'} \otimes |i\rangle_{B'} \otimes K_i$ (A' and B' belong to Alice and Bob, respectively, and K_i acts on B, the same system as that of σ) to σ. Then, for both Alice and Bob, who have no access to B' and A', respectively, system B is uncorrelated to their primed systems (A' and B') and system B is in the rank-d uniformly mixed state Φ_B. (See the proof of Theorem 1.)

Then, by applying the optimal d^2-dimensional dephasing unitary operator given in Ref. [19], which uses state Φ_B as a catalyst and applies the unitary operator $\sum_i |i\rangle\langle i|_A \otimes U_i$ to AB, where $\{U_i\}_{i=1}^{d^2}$ is an arbitrary set of orthonormal unitary operators, i.e., $\mathrm{Tr}[U_i U_j^\dagger] = \delta_{ij} d$, we can realize a d^2-dimensional dephasing map with the leftover SOR $\kappa \equiv \sum_i \mathrm{Tr}[K_i \sigma K_i^\dagger]|i\rangle\langle i|$ and the SOR used in this process is transformed into $\Phi_B \otimes \kappa_{B'}$. Since $S_{\min}(\Phi_B \otimes \kappa_{B'}) \geqslant S_{\min}(\Phi_B) = \log_2 d$, this SOR can be used again for another d^2-dimensional dephasing map; therefore, σ was used catalytically in this process. ∎

The catalyst used in this process has transformed from σ to $\Phi_B \otimes \kappa_{B'}$. We remark however that the catalyst's min-entropy never decreases during the process. This follows from, for all i,

$$2^{-S_{\min}(\Phi_B \otimes \kappa_{B'})} = \max_i \frac{1}{d}\mathrm{Tr}[K_i \sigma K_i^\dagger] \leqslant 2^{-S_{\min}(\sigma)}, \quad (10)$$

where the first equality follows from $2^{-S_{\min}(\Phi_B \otimes \kappa_{B'})}$ being the largest eigenvalue of $\Phi_B \otimes \kappa_{B'}$ and the second inequality follows from $\sigma \leqslant 2^{-S_{\min}(\sigma)}\mathbb{1}$ and $K_i^\dagger K_i \leqslant \Pi_{\mathrm{supp}(K_i)}$, where $\Pi_{\mathrm{supp}(K_i)}$ is the orthogonal projector onto the support of K_i (the orthogonal complement of the kernel of K_i) and $\mathrm{Tr}\Pi_{\mathrm{supp}(K_i)} = d$. Thus no consumption of randomness in terms of min-entropy happens in the process.

One can even recover full catalycity, if decoherence is allowed, by applying the controlled unitary to $\Phi_B \otimes \kappa_{B'}$ given as $\sum_i U_i^\dagger \otimes |i\rangle\langle i|$ with the unitary operators $\{U_i\}$ of the proof of Theorem 1 and discarding the latter system. This is because $\sum_i \mathrm{Tr}[K_i \sigma K_i^\dagger] U_i^\dagger \Phi_B U_i = \sigma$. Therefore, as it was assumed in [32], if $\kappa_{B'}$ undergoes decoherence and is dephased with respect to a basis unbiased from its eigenbasis, we can see that the catalyst returns to its original form σ with some uncorrelated leftover SOR, the state κ after being dephased.

On the other hand, if one wants to remove the leftover SOR κ completely to follow the conventional formalism of catalytic quantum randomness [19], note that a simple projective measurement on κ will collapse it into a pure state and leave the system A in the dephased state without the leftover

SOR (up to local unitary) and the catalyst in the state Φ_B, which is the standard form of catalyst [19], *deterministically*, regardless of the measurement outcome. This is because both $\kappa_{A'}$ and $\kappa_{B'}$ are completely decoupled from systems A and B, respectively. In this sense, one can say that the initial catalyst σ was actually a *precatalyst*, a compound that is converted into a catalyst during the chemical reaction, since it produces the true catalyst Φ_B in the course of interaction.

VI. CONCLUSION

Weak randomness sources with a nonuniform probability distribution often cause a nonzero probability of failure [33], sometimes to an irremediable extent [30,31] when their distribution is not fixed. We showed, however, for a fixed source of randomness or entanglement, that imperfect resources can yield deterministic security when their min-entropy is larger than the size of the secret they are hiding.

Aside from the results on quantum information processing tasks, we showed the power of nonuniform randomness sources as a catalyst, which could be interpreted as a thermal machine [18] in a quantum thermodynamics context, when it comes to state transition. By utilizing the Nielsen theorem [16], which was initially applied to entanglement extraction, we showed that nonuniform randomness sources can also serve as a catalyst and provided a necessary and sufficient condition for when it is possible. A dephasing map can also be understood as a quantum masking process of an observable. Our result shows that the randomness cost of masking one observable is half of the cost of masking all the quantum information in a system. This result solidifies the intuition that the information of one observable amounts to half of the quantum information in the same system.

Anticipated future work is to extend this result for arbitrary mixed quantum one-time pads. Unlike the results for safe states and SORs for dephasing maps, the result given in this work is not fully general for quantum one-time pads since we only considered pure quantum one-time pads.

ACKNOWLEDGMENTS

This work was supported by the National Research Foundation of Korea through grants funded by the Ministry of Science and ICT (Grants No. NRF-2019M3E4A1080074 and No. NRF-2020R1A2C1008609) via the Institute of Applied Physics at Seoul National University and the ITRC (Information Technology Research Center) support program (No. IITP-2021-2020-0-01606) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation).

[1] A. Steane, Proc. R. Soc. London A **452**, 2551 (1996).
[2] D. A. Lidar and T. A. Brun, *Quantum Error Correction* (Cambridge University Press, Cambridge, 2013).
[3] D. Gottesman, Phys. Rev. A **61**, 042311 (2000).
[4] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
[5] K. Modi, A. K. Pati, A. Sen(De), and U. Sen, Phys. Rev. Lett. **120**, 230501 (2018).
[6] M.-S. Li and K. Modi, Phys. Rev. A **102**, 022418 (2020).
[7] M.-S. Li and Y.-L. Wang, Phys. Rev. A **98**, 062306 (2018).
[8] B. Schumacher and M. D. Westmoreland, Phys. Rev. A **74**, 042305 (2006).
[9] F. G. S. L. Brandão and J. Oppenheim, Phys. Rev. Lett. **108**, 040504 (2012).
[10] A. Rényi, in *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics*, edited by J. Neyman (Regents of the University of California, Berkeley, 1961).
[11] M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel, J. Math. Phys. **54**, 122203 (2013).
[12] H. Imai, J. Müller-Quade, A. C. Nascimento, P. Tuyls, and A. Winter, Quantum Inf. Comput. **5**, 69 (2005).
[13] S. H. Lie, H. Kwon, M. Kim, and H. Jeong, Quantum **5**, 405 (2021).
[14] M. Hayashi, *Quantum Information Theory: Mathematical Foundation* (Springer, Berlin, 2017).
[15] S. H. Lie and H. Jeong, Phys. Rev. A **101**, 052322 (2020).
[16] M. A. Nielsen, Phys. Rev. Lett. **83**, 436 (1999).
[17] G. Gour, M. P. Müller, V. Narasimhachar, R. W. Spekkens, and N. Y. Halpern, Phys. Rep. **583**, 1 (2015).
[18] M. P. Müller, Phys. Rev. X **8**, 041051 (2018).
[19] P. Boes, H. Wilming, R. Gallego, and J. Eisert, Phys. Rev. X **8**, 041016 (2018).
[20] X.-B. Liang, B. Li, and S.-M. Fei, Phys. Rev. A **100**, 030304(R) (2019).
[21] A. Nayak and P. Sen, Quantum Inf. Comput. **7**, 103 (2007).
[22] M.-D. Choi, Linear Algebra Appl. **10**, 285 (1975).
[23] A. Jamiołkowski, Rep. Math. Phys. **3**, 275 (1972).
[24] S. L. Braunstein and A. K. Pati, Phys. Rev. Lett. **98**, 080502 (2007).
[25] M. J. Donald, M. Horodecki, and O. Rudolph, J. Math. Phys. **43**, 4252 (2002).
[26] G. Gour, Phys. Rev. A **70**, 042301 (2004).
[27] J. Scharlau and M. P. Mueller, Quantum **2**, 54 (2018).
[28] A. Horn, Am. J. Math. **76**, 620 (1954).
[29] S. H. Lie and H. Jeong, Phys. Rev. Research **3**, 013218 (2021).
[30] J. L. McInnes and B. Pinkas, in *CRYPTO 1990: Proceedings of the Conference on the Theory and Application of Cryptography*, edited by A. J. Menezes and S. A. Vanstone, Lecture Notes in Computer Science Vol. 537 (Springer, Berlin, 1991), pp. 421–435.
[31] Y. Dodis, S. J. Ong, M. Prabhakaran, and A. Sahai, in *Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science* (IEEE, Washington, DC, 2004), pp. 196–205.
[32] P. Boes, J. Eisert, R. Gallego, M. P. Müller, and H. Wilming, Phys. Rev. Lett. **122**, 210402 (2019).
[33] J. von Neumann, Various techniques used in connection with random digits, Natl. Bur. Stand. (U.S.) Appl. Math. Ser. No. 12 (U.S. GPO, Washington, DC, 1951), pp. 36–38.