Randomness cost of masking quantum information and the information conservation law

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

(Received 22 November 2019; accepted 20 April 2020; published 14 May 2020)

Masking quantum information, which is impossible without randomness as a resource, is a task that encodes quantum information into the bipartite quantum state while forbidding local parties from accessing that information. In this paper, we disprove the geometric conjecture about unitarily maskable states [Modi, Pati, Sen, and Sen, Phys. Rev. Lett. **120**, 230501 (2018)], and make an algebraic analysis of quantum masking. First, we show a general result of quantum channel mixing that a subchannel's mixing probability should be suppressed if its classical capacity is larger than the mixed channel's capacity. This constraint combined with the well-known *information conservation law*, a law that does not exist in classical information theories, gives a lower bound of randomness cost of masking quantum information as a monotone decreasing function of evenness of information distribution. This result provides a consistency test for various scenarios of fast scrambling conjecture on the black-hole evaporation process. Our results are robust to incompleteness of quantum masking.

DOI: 10.1103/PhysRevA.101.052322

I. INTRODUCTION

How can one hide information from two parties holding one's containers? Naïvely, one can tear the piece of paper containing the information into two pieces and distribute them to two parties so that it remains recoverable when the pieces are gathered together at a later point in time. However, this method leaks some amount of information to each party. To hide n bits of classical information completely, one needs to get n bits of classical information ("randomness") maximally correlated with it, for example, by using a one-time pad cipher [1]. Is it possible to hide n qubits of quantum information by making n qubits quantumly correlated with it? The no-hiding theorem and the no-masking theorem answer this question negatively for the pure state case [2,3]. In our previous work, we showed that one still needs additional n bits of randomness to hide n qubits of quantum information [4]. Results of [4] imply that different types of quantum correlation allowed in quantum masking processes require different amounts of randomness consumption, but the exact relation is still an open problem.

In this paper, we illuminate an information theoretical reason behind these phenomena and specify the backbone of the mechanism: the *information conservation law* of quantum mechanics. The information theoretical investigation yields a lower bound of the amount of randomness required for the information masking task in terms of a measure of how unevenly information is distributed between the system and the environment. This suggests that the important quantity for determining the minimal randomness consumption is not the exact amount of quantum correlation allowed between two parties but the unevenness of information distribution between two parties. Our result has implications for quantum secret sharing protocols and a class of proposals for resolving the black-hole information paradox called *scrambling* [5].

Let $\mathcal{B}(\mathcal{H})$ be the space of operators on a finite-dimensional Hilbert space $\mathcal{H}$ and let $\mathfrak{S}(\mathcal{H})$ be the set of quantum states on the Hilbert space $\mathcal{H}$. A *masking process* or *quantum masker* [3,4] $\Phi_M : \mathcal{B}(\mathcal{H}_Q) \to \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$ hiding a set $\Lambda \subset \mathfrak{S}(\mathcal{H}_Q)$ of quantum states is an invertible quantum map [a completely positive trace preserving (CPTP) map the inverse of which is also a CPTP map] that has constant marginal states for inputs from Λ, i.e.,

$$\forall \rho \in \Lambda, \quad \mathrm{Tr}_B \Phi_M(\rho) = \sigma_A, \quad \text{and} \quad \mathrm{Tr}_A \Phi_M(\rho) = \sigma_B, \tag{1}$$

namely, a quantum masker distributes a quantum state to two parties so that each party has no access to any information about the original quantum state. When $\Lambda = \mathfrak{S}(\mathcal{H}_Q)$, the masker is called *universal* and if the masker maps the pure state to the pure state then it is called *unitary* or *isometry*. Its invertibility allows the following expression [6]:

$$\Phi_M(\rho) = M(\rho_Q \otimes \sigma_S)M^\dagger, \tag{2}$$

with some isometry $M : \mathcal{H}_Q \otimes \mathcal{H}_S \to \mathcal{H}_A \otimes \mathcal{H}_B$ and a quantum state σ_S. We call the state σ_S the *safe state* of the masking process and we interpret it as a quasiclassical randomness source that is needed to mask the quantum information. One can interpret the von Neumann entropy of safe state σ_S as the *randomness cost* $\mathcal{R}(\Phi_M)$ of Φ_M, which is defined for any pure state $|\phi\rangle \in \mathcal{H}_Q$:

$$\mathcal{R}(\Phi_M) := S[\Phi_M(|\phi\rangle\langle\phi|_Q)] = S(\sigma_S), \tag{3}$$

where S is the von Neumann entropy. Our interest is to investigate the relation between the randomness cost of the masking process and the characteristics of quantum interaction M of the process. The following result on the size of each party is known [4,7,8]. Hereinafter, log denotes the logarithmic function with base 2.

Fact 1: The generalized quantum masking theorem. For a universal quantum masker $\Phi_M : \mathcal{B}(\mathcal{H}_Q) \to \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$

*h.jeong37@gmail.com

with constant marginal states σ_A and σ_B for systems A and B and the safe state σ_S, we have

$$\min\{S(\sigma_A), S(\sigma_B), S(\sigma_S)\} \geqslant \log_2 \dim(\mathcal{H}_Q).$$

If $\sigma_S = \sum_i p_i |i\rangle\langle i|_S$ is the spectral decomposition of σ_S, then Φ_M can be expressed as a random isometry operation:

$$\Phi_M(\rho) = \sum_i p_i M_i \rho M_i^\dagger, \tag{4}$$

where $M_i := M(\mathbb{1}_Q \otimes |i\rangle_S)$ are isometries from $\mathcal{H}_Q$ to $\mathcal{H}_A \otimes \mathcal{H}_B$. We will call such isometry a *bipartite embedding*. These isometries also have orthogonal images ($M_i^\dagger M_j = 0$ if $i \neq j$). Such decomposition of Φ_M is unique up to degeneracy of the spectrum of the safe state σ_S.

In quantum information theory, there is a unique conservation law of information in contrast with classical information theory. When an entangled state $|\Psi\rangle_{\mathrm{RQ}}$ undergoes an arbitrary isometry $U : \mathcal{H}_Q \to \mathcal{H}_A \otimes \mathcal{H}_B$, then the system R's mutual information with two output systems A and B is conserved in the following sense. One can consider that system R is the reference system of system Q.

Fact 2: Information conservation law.

$$2S(R) = I(R : A) + I(R : B). \tag{5}$$

We note that this simple law alone can derive both the *no-hiding theorem* [2] and the *no-masking theorem* [3]. If the bipartite embedding $U : \mathcal{H}_Q \to \mathcal{H}_A \otimes \mathcal{H}_B$ is a hiding or masking process so that output system A is in a constant quantum state regardless of the input state of system Q, then for a maximally entangled state $|\Gamma\rangle_{\mathrm{RQ}}$ with $\dim(\mathcal{H}_Q) = \dim(\mathcal{H}_R) = d$ we have $I(R : A) = 0$ as systems R and A are in a product state. But this immediately implies $I(R : B) = 2\log_2 d > 0$. This implies that there is no bipartite embedding that can hide quantum information from both parties. From this observation we can expect the information conservation law could give an insight on the generalized quantum masking theorem.

We can interpret $I(R : A)$ as the information flow from Q to A when $\mathrm{Tr}_B(U \cdot U^\dagger)$ is considered a channel from Q to A. We can intuitively anticipate that if too much information has flowed to a single system then a large amount of randomness is needed to "scramble" to mask that information, just as it is for the classical one-time pad cipher. In the following section, we first prove an easily applicable result that verifies this intuition from simple entropic properties, and again prove a stronger theorem from an information-theoretic argument.

II. MAIN RESULTS

A. Unitarily maskable set conjecture

From now on, we will call a masking process $\Phi_M : \mathcal{B}(\mathcal{H}_Q) \to \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$ d dimensional if the states being masked by it are d dimensional, i.e., if $d = \dim(\mathcal{H}_Q)$. After that, we will fix a d-dimensional universal quantum masker Φ_M and its bipartite embedding decomposition $\Phi_M(\rho) = \sum_i p_i M_i \rho M_i^\dagger$. Also every entropic quantity with subscript i refers to the corresponding quantity for the pure state $(\mathbb{1}_R \otimes M_i)|\Gamma\rangle_{\mathrm{RQ}}$ of the tripartite system RAB and unindexed entropic quantities such as $S(X)$ are the corresponding values for system X in the state $(\mathbb{1}_R \otimes \Phi_M)(|\Gamma\rangle\langle\Gamma|_{\mathrm{RQ}})$ of the tripartite system RAB. For every quantum channel $\mathcal{N}$ into $\mathcal{H}_A \otimes \mathcal{H}_B$, we will denote its partial traces as $\mathrm{Tr}_B \circ \mathcal{N} = \mathcal{N}^A$ and $\mathrm{Tr}_A \circ \mathcal{N} = \mathcal{N}^B$.

We first investigate the power of the isometry quantum masker by disproving the conjecture given in [3].

Conjecture 1: Modi et al. [3]. For every isometry quantum masker $\mathcal{M}(\cdot) = M \cdot M^\dagger : \mathcal{B}(\mathcal{H}_Q) \to \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{B}(\mathcal{H}_B)$ with $m = \dim(\mathcal{H}_Q)$, its set of maskable states is in a "disk," i.e., the convex hull of a set of states $\{|\psi\rangle\langle\psi| : |\psi\rangle = \sum_{k=1}^m r_k e^{i\theta_k}|k\rangle, \theta_k \in [-\pi, \pi]\}$ with fixed non-negative real numbers r_k such that $\sum_k r_k^2 = 1$ and a fixed orthonormal basis $\{|k\rangle\}_{k=1}^m$.

We give a counterexample that disproves this conjecture. Consider a qudit-qudit system $\mathcal{H}_Q$, that is, $\dim(\mathcal{H}_Q) = d^2$, and an isometry masking process $\mathcal{M}$ which is simply distributing a qudit to each party. Note that this masking process is essentially equivalent to any masking process from a d^2-dimensional system to two d-dimensional parties since any d^2-dimensional unitary applied before the distribution only amounts to a change of basis.

Now, consider the set W of bipartite states that has maximally mixed states as its marginal states. This is a set of maskable states of the masking process $\mathcal{M}$ given above.

Assuming Conjecture 1, suppose that there exists a basis $\{|T_k\rangle\}_{k=1}^{d^2}$ of $\mathcal{H}_Q$ such that every state in W has the same diagonal element with respect to this basis. This implies that for any local basis $\{|a_j\rangle\}_{j=1}^d$ and $\{|b_j\rangle\}_{j=1}^d$ of $\mathcal{H}_\mathcal{A}$ and $\mathcal{H}_\mathcal{B}$, respectively, the following constraint is required with varying phases $\theta_j \in [-\pi, \pi]$ for any $1 \leqslant j \leqslant d$:

$$\frac{1}{d}\left|\sum_j e^{i\theta_j}\langle T_k|(|a_j\rangle \otimes |b_j\rangle)\right|^2 = \text{const}, \tag{6}$$

for every $1 \leqslant k \leqslant d^2$. This follows from the fact that $\frac{1}{\sqrt{d}}\sum_j e^{i\theta_j}|a_j\rangle \otimes |b_j\rangle$ is in W for any local bases $\{|a_j\rangle\}_{j=1}^d$ and $\{|b_j\rangle\}_{j=1}^d$ and phases $\{\theta_j\}_{j=1}^d$.

If $|T_k\rangle$ is not a product state, then one can violate the constraint above by picking the Schmidt bases of $|T_k\rangle$ as local bases. This is because, when $s_i^{(k)} \geqslant 0$ are Schmidt coefficients of $|T_k\rangle$, $\frac{1}{d}|\sum_j e^{i\theta_j} s_j^{(k)}|$ cannot be constant with varying phases θ_j if more than one $s_j^{(k)}$ are nonzero. Therefore $\{|T_k\rangle\}_{k=1}^{d^2}$ is a product basis of the form $|T_{d(i-1)+j}\rangle = |\alpha_i\rangle_A|\beta_j\rangle_B$ for some local bases $\{|\alpha_j\rangle\}_{j=1}^d$ and $\{|\beta_j\rangle\}_{j=1}^d$. However, requiring the constraint above again for the discrete Fourier-transformed local bases $\{|\tilde{\alpha}_j\rangle := \sum_l \frac{1}{\sqrt{d}} e^{i2\pi jl/d}|\alpha_l\rangle\}_{j=1}^d$ (and similarly defined $\{|\tilde{b}_j\rangle\}_{j=1}^d$) leads to the violation of the constraint. Therefore there exists no such basis $\{|T_k\rangle\}_{k=1}^{d^2}$.

This suggests that information hidden by a quantum masking process exploiting the inherent multipartite structure of a quantum state (e.g., interpreting a four-level system as a two-qubit system) need not be limited to the phase information with respect to a certain "classical" basis. In fact, any kind of correlation between two subsystems (be it quantum or classical) could be hidden when these two subsystems are separate.

B. Randomness cost of quantum masking

The information conservation law suggests that at least $\log_2 d$ bits of information should leak to at least one party, but our counterexample suggests that $\log_2 d$ bits of information need not correspond to the classical information with respect to some preferred basis. Indeed, the information could correspond to quantum information of a $\sqrt{d}$-dimensional quantum system. We are left in the situation in which there is no convenient geometrical tool to analyze the masking power of each isometry quantum masker, i.e., bipartite embedding. Thus the information conservation law (5) is the best principle one could rely on. By using some simple entropic properties, we can first derive the following preliminary result about quantum masking processes consuming randomness. Proofs of the theorems in the following sections can be found in the Appendix.

Theorem 1. For any universal quantum masker Φ_M and any set of its bipartite embeddings $\{M_i\}$,

$$\max_{X\in\{A,B\}} \sum_i p_i I(R:X)_i \leqslant \mathcal{R}(\Phi_M).$$

This result already implies the generalized quantum masking theorem since $\max_{X\in\{A,B\}} \sum_i p_i I(R:X)_i \geqslant \log_2 d$ as $\sum_i p_i I(R:A)_i + \sum_i p_i I(R:B)_i = 2\log_2 d$ from the information conservation law.

However, often the lower bound above is not enough for many quantum maskers. A more detailed result can be obtained by observing that quantum masking process consuming randomness can be considered a channel mixing process. We can derive the following tradeoff relation between the channel capacity of a subchannel and its mixing probability.

Theorem 2. Let a quantum channel $\mathcal{N}$ be given as a convex sum of subchannels $\{\mathcal{N}_i\}$, i.e., $\sum_i p_i\mathcal{N}_i = \mathcal{N}$. Then for all i the difference of the entanglement-assisted classical capacity C_{EA} of $\mathcal{N}_i$ and $\mathcal{N}$ is upper bounded by the information content of the randomness source for its corresponding i, i.e.,

$$C_{\mathrm{EA}}(\mathcal{N}_i) - C_{\mathrm{EA}}(\mathcal{N}) \leqslant -\log_2 p_i. \tag{7}$$

Note that actually the proof of the theorem above can be applied to the classical capacity of the quantum channel with any kind of proper resource assumption, not necessarily the unboundedness of predistributed entanglement.

From the fact [9,10] that for any quantum channel $\mathcal{N}: A' \to B$

$$\max_{\phi_{AA'}} I(A:B)_{\tau_{AB}} = C_{\mathrm{EA}}(\mathcal{N}), \tag{8}$$

where $\phi_{AA'}$ is a pure state on AA' and $\tau_{AB} = (\mathbb{1}_A \otimes \mathcal{N}_{A'\to B})(\phi_{AA'})$, we have the following corollary,

$$\max\{I(R:A)_{\tau_{RA}}, I(R:B)_{\tau_{RB}}\} \leqslant -\log_2 p_i, \tag{9}$$

for an arbitrarily given bipartite pure state ϕ_{RQ} with $\tau_{\mathrm{RAB}} = (\mathbb{1}_R \otimes \Phi_i)(\phi_{\mathrm{RQ}})$. Choosing arbitrary maximally entangled state ϕ_{RQ} and averaging both sides of (9) leads to the following result.

Corollary 1. For any d-dimensional universal quantum masker Φ_M with the safe state with spectrum $\{p_i\}$, the following inequality holds:

$$\log_2 d + \sum_i p_i |S(A)_i - S(B)_i| \leqslant \mathcal{R}(\Phi_M). \tag{10}$$

Corollary 1 can be considered a combination of two results. First, higher information influxes should be scrambled with a larger amount of randomness if their net influx should be suppressed under a certain value. Second, information cannot be destroyed or hidden under unitary interaction; it flows either to the system or to the environment. Therefore, a set of unitary interactions that allow information flow to each party to be more even requires a smaller amount of randomness to form a quantum masking process.

It is worth defining a measure of evenness of information distribution between two parties that only depends on the set of bipartite embeddings. Consider a measure defined in the following way with the notation $I_i := \max\{I(R:A)_i, I(R:B)_i\}$:

$$\mathcal{I}_1(\{M_i\}_{i\in I}) := \max_{|\Gamma\rangle} \min_{S\subseteq I} H\left(\left\{\frac{1}{2^{I_i}}\right\}_{i\in S}\right), \tag{11}$$

where $H(\{t_i\}_{i\in T}) := -\sum_{i\in T} t_i \log_2 t_i$ is formally defined as the Shannon entropy even for the set of non-negative numbers $\{a_i\}_{i\in T}$ that is not a probability distribution. The maximization is over the choice of initial bipartite pure state $|\Gamma\rangle_{\mathrm{RQ}}$ and the minimization is over the subset of indices $S \subseteq I$ such that $\sum_{i\in S} 2^{-I_i} \geqslant 1$ with existence of $i_0 \in S$ such that $\sum_{i\in S} 2^{-I_i} - 2^{-I_{i_0}} \leqslant 1$. Since $\mathcal{I}_1$ is a monotone increasing function of $\max\{I(R:A)_i, I(R:B)_i\}$ for each i and each $I_i = \log_2 d + |S(A)_i - S(B)_i|$ signifies how unevenly information flows to A and B when the bipartite embedding M_i is applied, $\mathcal{I}_1$ is a legitimate measure of information unevenness. $\mathcal{I}_1$ is bounded as $\log_2 d \leqslant \mathcal{I}_1 \leqslant 2(1+d^{-1})\log_2 d$.

Once the one-shot measure $\mathcal{I}_1$ is defined, one can define its regularized version $\mathcal{I}_\infty(\{M_i\}) := \lim_{n\to\infty} \frac{1}{n}\mathcal{I}_1(\{M_i\}^{\otimes n})$. This regularized measure has the bound of $\log_2 d \leqslant \mathcal{I}_\infty \leqslant 2\log_2 d$. We have the following lower bound of the randomness cost of the quantum masking process that is a monotone decreasing function of evenness of information distribution thereof.

Theorem 3. For any d-dimensional universal quantum masking process Φ_M composed of random bipartite embeddings $\{M_i\}_{i\in I}$ with orthogonal images, the following inequality holds:

$$\mathcal{I}_\infty(\{M_i\}_{i\in I}) \leqslant \mathcal{R}(\Phi_M). \tag{12}$$

It is worth noting that Theorem 3 can be saturated (e.g., quantum one-time pads [11] and four-qubit maskers [4]). An important implication of the inequality above, which is highlighted in the difference between the naïve Theorem 1 and the more refined Corollary 1 and Theorem 3, is that the most relevant property of the masking interaction is not the mean information flow, but the mean *evenness of information flow*. For example, for a hiding process in which information entirely flows to system A with the total probability of $1/2$ and vice versa for system B, the mean information flow for each system is the same. However, the evenness of information flow is at a minimum in any subchannel, therefore this process requires at least $2\log_2 d$ bits of randomness for masking d-dimensional quantum information.

The measure $\mathcal{I}_1(\{M_i\}_{i\in I})$ can be interpreted as the randomness cost of a masking process that can be formed by mixing bipartite embeddings from $\{M_i\}_{i\in I}$ with the probability assignment that assigns as much probability as possible to the bipartite embeddings with the most even information flow. Such a strategy is optimal for minimizing randomness cost since bipartite embeddings with evener information flow themselves can hide more information even before being mixed and they also can take up larger probability according to Theorem 2. $\mathcal{I}_\infty(\{M_i\}_{i\in I})$ can be useful since the aforementioned probability assignment can lead to an incomplete probability distribution, but employing the same assignment strategy for the tensor product of the given set of bipartite embeddings results in an incomplete probability distribution that is closer to a complete one. Note that concentrating probability to a small set can decrease the overall randomness. Discrepancy between this value and the real randomness cost can happen if the bipartite embeddings with the most even information flows have been poorly chosen so that they do not effectively cancel each other.

One possible issue of randomness usage in the quantum information process is the nonuniformity of the randomness source. However, typicality of the random state [12] asserts that one could treat many copies of a nonuniform random state as a single uniform random state when one can permit a small error. The robustness of Theorem 2 guarantees the robustness of the inequalities above, as one can substitute all I_i terms with $I_i - e$ for the nonperfect masking case with the entanglement-assisted classical capacity e. Therefore the results shown here are compatible with other analyses on random quantum processes that use uniform randomness exclusively [4,13].

It is impossible to delete quantum information [14]. Therefore, to hide information from one system, unless one just displaces quantum information to another system, one needs to "cancel out" the information by randomly altering the information. What Theorem 2 says is that a large amount of information leakage requires a large amount of randomness to conceal it. From this one might speculate that the presence of a single "large" information leakage subchannel may require a large amount of randomness to scramble it, i.e.,

$$\max_{X\in\{A,B\},i} I(R:X)_i \overset{?}{\leqslant} \mathcal{R}(\Phi_M). \tag{13}$$

The following example, however, disproves this speculation. A subchannel with high channel capacity need not be canceled by other highly randomized subchannels with equally high channel capacity, if partial distribution of quantum information to two parties is allowed. Note that we still have $\min_i \max_{X\in\{A,B\}} I(R:X)_i \leqslant \mathcal{R}(\Phi_M)$ nonetheless.

Consider the following families of bipartite embeddings $\mathcal{H}_Q \to \mathcal{H}_A \otimes \mathcal{H}_B$, defined on a d-dimensional Hilbert space $\mathcal{H}_Q$ with *odd* number d. For an input state $|\psi\rangle_I = \sum_{i=1}^d \alpha_i |i\rangle_I$ with fixed bases $\{|i\rangle_X\}$ for each $X \in \{A, B, I\}$, $M_{A,i}|\psi\rangle_I := (Z^i|\psi\rangle_A) \otimes |i+d\rangle_B$, $M_{B,i}|\psi\rangle_I := |i+d\rangle_A \otimes (Z^i|\psi\rangle_B)$, for $1 \leqslant i \leqslant d$ and $M_j|\psi\rangle_I := \sum_i \alpha_i |i \oplus j\rangle_A \otimes |i \oplus 2j\rangle_B$, where $\oplus$ stands for modular sum modulo d for $1 \leqslant j \leqslant d-1$.

One can observe that $M_{A,i}$ and $M_{B,i}$ are bipartite embeddings with completely uneven information flow but M_j has even flow. These bipartite embeddings with a safe state $\sigma_S := \sum_{i=1}^d \frac{1}{d(d+1)} |A,i\rangle\langle A,i|_S + \sum_{i=1}^d \frac{1}{d(d+1)} |B,i\rangle\langle B,i|_S + \sum_{j=1}^{d-1} \frac{1}{d+1} |j\rangle\langle j|_S$ form a universal quantum masker with $\mathcal{R} = \log_2(d+1) + \frac{2}{d+1}\log_2 d$. Although $\max_i I(R:X)_i = 2\log_2 d$, we have $\mathcal{R} < 2\log_2 d$ for all $d \geqslant 2$. However, the bound above almost sharply captures the randomness cost with the small gap of $\mathcal{R} - \mathcal{I}_1 = \log_2(1+d^{-1}) - \frac{d-1}{d(d+1)}\log_2 d$ that approaches zero as $d \to \infty$.

III. DISCUSSION

A. Sharing the quantum secret without attending

For every quantum masker Φ_M, its safe state σ_S's purification system K (meaning that there exists a bipartite pure state $|\Sigma\rangle_{SK}$ such that $\mathrm{Tr}_K|\Sigma\rangle\langle\Sigma|_{SK} = \sigma_S$) automatically shares its share of the quantum secret generated from a (2,3)-threshold quantum secret sharing scheme [15], without interacting with either of the systems S and Q. Here the quantum secret is the quantum information that has been masked. This statement means that either of two groups of parties, AK or BK, can restore the quantum information that was masked without help of the other party. This is a direct result of the no-hiding theorem [2], which states that if the quantum information is hidden from one party then it should be isometrically transferred to the remaining parties.

In the quantum masking scenario, if the quantum information is hidden from, say, system A, it is isometrically transferred to systems BK, which allows them to restore the quantum information directly. This observation implies that initially distributed entanglement has the ability to transfer a share of the quantum secret generated at a later point in time, and the inequality derived in this paper gives the lower bound on the amount of entanglement in terms of the property of interactions used in the masking process. This observation yields an insight on the process of black-hole evaporation discussed in the next section.

We remark that this observation allows us to estimate the sizes of unauthorized sets of not only the (2,3)-threshold quantum secret sharing protocol but also any pure $(k, 2k-1)$-threshold protocol with our result. This follows from the observation that partitioning $2k-1$ parties into any three unauthorized sets yields the (2,3)-threshold quantum secret sharing protocol. This lower bound is stronger than the previously known $\log_2 d$ bound [8] and admits estimation of sizes of unauthorized systems for nonperfect quantum secret sharing protocols from the robustness against error.

B. Black-hole evaporation

Hawking's semiclassical analysis [16,17] of the outgoing radiation from a black hole indicates that the flow of particles from a black hole should contain no information related to in-fallen matter. In addition, information cannot be stored in the black hole because it can be vanished at the final stage of its evaporation. This is impossible unless quantum information can be lost, which is forbidden by the unitarity of quantum mechanics. From these observations one could conclude that the information of in-fallen matter should be "masked" into the correlation between the black hole and the Hawking radiation thereof. Since there is no limitation to the

quantum state of in-fallen matter, the hypothetical masking process, if any, should be universal. However, the no-masking theorem says that this is impossible if the masking process is unitary. This paradox is called the *black-hole information paradox*.

A possible resolution of the black-hole information paradox is fast scrambling in a black hole [5]. Once a black hole starts in a pure quantum state and if the time evolution after its creation is unitary, then the black hole's internal state is always entangled with the Hawking radiation it has emitted. It is believed that after the Page time [18] of the given black hole the black hole's internal state is nearly maximally entangled with all the Hawking radiation that has been radiated up to that point. The analysis in [5] suggests that in this scenario any k qubit of information falling into the black hole can be almost perfectly retrieved by an observer who has access to all the Hawking radiation emitted from the black hole by acquiring just a little bit more Hawking radiation up to $k + c$ qubits where c is a constant that depends only on the desired error rate. In other words, black holes function as mirrors in the model.

The model depends on the *ad hoc* assumption of typical unitary evolution under Haar distribution of the black-hole internal state and the assumption that its entire surface participates in the scrambling process. This assumption, however, is not indispensable [19]. Our result here gives a way to examine the consistency between assumptions on scrambling and evaporation processes.

Here we suppose the internal interaction and evaporation process of a black hole as a quantum masking process since after the emission of k qubits through Hawking radiation either the black-hole internal state or the just radiated k qubits of emission should not have any information on the k qubits of the in-falling object. When written in the notations of Eq. (1), the in-falling object's system is Q, the black hole's internal state is that of system S, the in-falling Hawking radiation is A, and the outgoing Hawking radiation is B. Suppose that for a given moment parametrized by time T of a black hole's lifetime the internal interaction is determined by unitary M (with the accompanying set of bipartite embeddings $\{M_i := M(\mathbb{1} \otimes |i\rangle)\}_{i\in I}$,) from a hypothetical theory on the black-hole dynamics. From this, one can calculate $\mathcal{I}_\infty(\{M_i\}_{i\in I})$. Further, if the entropy of entanglement of the black hole (the contribution of which is dominant in the thermodynamic entropy of the black hole [20] without a firewall [21]) for the given moment is $S(T)$, and only a $c(t^*)$ fraction ($0 \leqslant c \leqslant 1$) of the black-hole surface can participate for the given scrambling time t^*, then we have the following relation:

$$\mathcal{I}_\infty(\{M_i\}_{i\in I}) \leqslant c(t^*)S(T). \tag{14}$$

Even without explicit calculation of $\mathcal{I}_\infty(\{M_i\}_{i\in I})$, one already has the relation between the reflection capacity of the black hole and its entropy of entanglement at the moment from the trivial lower bound of $k \leqslant \mathcal{I}_\infty(\{M_i\}_{i\in I})$ where k is the number of qubits that can be scrambled at a time with given scrambling time t^*. In other words, in the early or late stage of a black hole's evolution (i.e., S is small) the black hole should have very small reflection capacity. This relation provides a way to check consistency between quantities determined from independent theories such as scrambling time, internal evolution of a black hole, and time evolution of the entropy of entanglement of a black hole. Especially, when the internal interaction of a black hole is inherently asymmetric (e.g., information only "heads" outward through radiation as it is proposed in [20] as quantum one-time pad encoding of in-fallen information or information always coherently "falls" into the horizon for each bipartite embedding) the upper bound of the reflection capacity of a black hole can drop up to half of the entropy of entanglement of the black hole.

Note added. We recently learned of the independent result of Ding and Hu [22] on counterexamples of Conjecture 1 for the qutrit unitary quantum masker. We remark that the counterexample in the present paper forms a different family of quantum states from that of [22] as it is for $d \geqslant 4$-dimensional unitary quantum maskers.

ACKNOWLEDGMENTS

This work was supported by the National Research Foundation of Korea through grants funded by the Korea Government (Grants No. NRF-2019R1H1A3079890, No. NRF-2019M3E4A1080074, and No. NRF-2020R1A2C1008609).

APPENDIX: PROOF OF THE RESULTS

Theorem 1. For any universal quantum masker Φ_M and any set of its bipartite embeddings $\{M_i\}$,

$$\max_{X\in\{A,B\}} \sum_i p_i I(R:X)_i \leqslant \mathcal{R}(\Phi_M).$$

Proof. Without loss of generality, we can assume $X = A$. Then as $I(R:A)_i = S(R)_i + S(A)_i - S(B)_i = S(R) + S(A)_i - S(B)_i$ it suffices to prove the following inequality:

$$S(R) + \sum_i p_i S(A)_i \leqslant H(\{p_i\}) + \sum_i p_i S(B)_i, \tag{A1}$$

because $H(\{p_i\}) = S(\sigma_S)$, where $H(\{q_i\}) := -\sum_i q_i \log_2 q_i$ is the Shannon entropy of the probability distribution $\{q_i\}$. As $\sum_i p_i S(\rho_i) \leqslant S(\sum_i p_i \rho_i)$ from the concavity of von Neumann entropy [23], we have

$$S(R) + \sum_i p_i S(A)_i \leqslant S(R) + S(A) = S(RA), \tag{A2}$$

because systems R and A are in a product state because of the masking property of Φ_M. If we define $\Phi_i^A(\rho) := \mathrm{Tr}_B(M(\rho_I \otimes |i\rangle\langle i|_S)M^\dagger)$, $S(RA)$ equals to

$$S\left[\sum_i p_i (\mathbb{1}_R \otimes \Phi_i^A)(|\Gamma\rangle\langle\Gamma|_{\mathrm{RQ}})\right]. \tag{A3}$$

From the following property of von Neumann entropy [23],

$$S\left(\sum_i q_i \rho_i\right) \leqslant H(\{q_i\}) + \sum_i q_i S(\rho_i), \tag{A4}$$

we have

$$S(RA) \leqslant H(\{p_i\}) + \sum_i p_i S(RA)_i. \tag{A5}$$

This proves the wanted inequality since $S(RA)_i = S(B)_i$ because systems RAB are in a pure state. Since this inequality

holds for arbitrary maximally entangled state $|\Gamma\rangle_{\mathrm{RQ}}$, we have the wanted result. ■

Theorem 2. Let a quantum channel $\mathcal{N}$ be given as a convex sum of subchannels $\{\mathcal{N}_i\}$, i.e., $\sum_i p_i\mathcal{N}_i = \mathcal{N}$. Then for all i the difference of the entanglement-assisted classical capacity C_{EA} of $\mathcal{N}_i$ and $\mathcal{N}$ is upper bounded by the information content of the randomness source for its corresponding i, i.e.,

$$C_{\mathrm{EA}}(\mathcal{N}_i) - C_{\mathrm{EA}}(\mathcal{N}) \leqslant -\log_2 p_i. \tag{A6}$$

Proof. We first prove the case where $\mathcal{N}$ is a complete erasure channel $[C_{\mathrm{EA}}(\mathcal{N}) = 0]$. In this case, no information should be conveyed over $\mathcal{N}$. Assume that for some i

$$C_{\mathrm{EA}}(\mathcal{N}_i) > -\log_2 p_i. \tag{A7}$$

Then there exist $\epsilon, \delta > 0$ for all positive integers $n > 0$ such that

$$p_i^n(1-\delta) > \frac{1}{2^{n(1-\epsilon)C_{\mathrm{EA}}(\mathcal{N}_i)}}. \tag{A8}$$

We now consider an information transfer task between an encoder and a decoder. The encoder uniformly samples an arbitrary letter L from N possible candidates, then encodes and transfers it by using the channel $\mathcal{N}$ multiple times with the assistance of an unbounded amount of entanglement. Since $\mathcal{N}$ is a completely lossy channel, the decoder should have no information at all about the letter L. Therefore the probability of the decoder guessing the letter L correctly should never exceed $\frac{1}{N}$.

Nevertheless if the encoder and the decoder choose a strategy in which they always assume that the channel is $\mathcal{N}_i$ instead of $\mathcal{N}$, then because of the achievability theorem, with the probability that is no less than $p_i^n(1-\delta)$, the decoder can guess the letter L uniformly sampled from $2^{n(1-\epsilon)C_{\mathrm{EA}}(\mathcal{N}_i)}$ possible alphabets, by using the channel n times with sufficiently large n. However, as $p_i^n(1-\delta) > 2^{-n(1-\epsilon)C_{\mathrm{EA}}(\mathcal{N}_i)}$ from the assumption, this contradicts the previous statement.

Now, for the case of capacity $C_{\mathrm{EA}}(\mathcal{N})$, one can only have up to $2^{nC_{\mathrm{EA}}(\mathcal{N})}$-fold probability enhancement for correctly guessing the letter with the lowest probability, when using the channel n times, compared to the complete erasure channel case. But still negation of the assumption yields the existence of an index i for which positive ϵ and δ exist for any positive integer n such that

$$p_i^n(1-\delta) > \frac{2^{nC_{\mathrm{EA}}(\mathcal{N})}}{2^{n(1-\epsilon)C_{\mathrm{EA}}(\mathcal{N}_i)}}. \tag{A9}$$

This implies the existence of the strategy of Alice and Bob achieving a probability strictly higher than the maximum probability. ■

Theorem 3. For any d-dimensional universal quantum masking process Φ_M composed of random bipartite embeddings $\{M_i\}_{i\in I}$ with orthogonal images, the following inequality holds:

$$\mathcal{I}_\infty(\{M_i\}_{i\in I}) \leqslant \mathcal{R}(\Phi_M). \tag{A10}$$

Proof. We first prove the following seemingly weaker inequality:

$$\mathcal{I}_1(\{M_i\}_{i\in I}) \leqslant \mathcal{R}(\Phi_M) + \frac{2\log_2 d}{d}. \tag{A11}$$

From Corollary 1 of the main text,

$$\log_2 d + \sum_i p_i |S(A)_i - S(B)_i| \leqslant \mathcal{R}(\Phi_M), \tag{A12}$$

and the fact that $I_i = \log_2 d + |S(A)_i - S(B)_i|$, we have

$$\max_{|\Gamma\rangle} \min_{\{p_i\}} \sum_i p_i I_i \leqslant \mathcal{R}(\Phi_M), \tag{A13}$$

where the maximization is over every bipartite state $|\Gamma\rangle_{\mathrm{RQ}}$ and the minimization is over every possible probability distribution $\{p_i\}$ that satisfies $p_i \leqslant 2^{-I_i}$ for each i. When S is an index set that saturates the minimization in the definition of $\mathcal{I}_1(\{M_i\}_{i\in I})$,

$$\mathcal{I}_1(\{M_i\}_{i\in I}) = \max_{|\Gamma\rangle} \min_{S\subseteq I} H\left(\left\{\frac{1}{2^{I_i}}\right\}_{i\in S}\right), \tag{A14}$$

the minimization term in (A13) with such probability assignment is larger than the Shannon entropy $H(\{2^{-I_i}\}_{i\in S_0})$ with the index set $S_0 := S \setminus \{i_0\}$, because the probability distribution saturating the minimization in (A11) is assigning $p_i = 2^{-I_i}$ to indices in some S' with the lowest values of I_i until $\sum_{i\in S'} 2^{-I_i} \leqslant 1$ and assigning the probability $p_{i_0} = 1 - \sum_{i\in S'} 2^{-I_i}$ to the index with the next smallest I_{i_0} and the fact that $\{2^{-I_i}\}_{i\in S_0}$ is an incomplete probability distribution. Combined with the fact that any term $2^{-I_i}I_i$ is not larger than $2d^{-1}\log_2 d$, this yields the wanted result (A11). By noting that $\mathcal{R}(\Phi_M)$ is additive, that is, $\mathcal{R}(\Phi_M^{\otimes n}) = n\mathcal{R}(\Phi_M)$, regularizing both sides of (A11) yields (A10). ■

[1] C. E. Shannon, Bell Syst. Tech. J. **28**, 656 (1949).

[2] S. L. Braunstein and A. K. Pati, Phys. Rev. Lett. **98**, 080502 (2007).

[3] K. Modi, A. K. Pati, A. Sen(De), and U. Sen, Phys. Rev. Lett. **120**, 230501 (2018).

[4] S. H. Lie, H. Kwon, M. Kim, and H. Jeong, arXiv:1903.12304 (2019).

[5] P. Hayden and J. Preskill, J. High Energy Phys. 09 (2007) 120.

[6] A. Nayak and P. Sen, Quantum Inf. Comput. **7**, 103 (2007).

[7] D. Gottesman, Phys. Rev. A **61**, 042311 (2000).

[8] H. Imai, J. Müller-Quade, A. C. Nascimento, P. Tuyls, and A. Winter, Quantum Inf. Comput. **5**, 69 (2005).

[9] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, Phys. Rev. Lett. **83**, 3081 (1999).

[10] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, IEEE Trans. Inf. Theory **48**, 2637 (2002).

[11] M. Mosca, A. Tapp, and R. de Wolf, arXiv:quant-ph/0003101 (2000).

[12] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley, New York, 2012).

[13] P. Boes, H. Wilming, R. Gallego, and J. Eisert, Phys. Rev. X **8**, 041016 (2018).
[14] A. K. Pati and S. L. Braunstein, Nature (London) **404**, 164 (2000).
[15] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
[16] S. W. Hawking, Nature (London) **248**, 30 (1974).
[17] S. W. Hawking, Commun. Math. Phys. **43**, 199 (1975).
[18] D. N. Page, Phys. Rev. Lett. **71**, 3743 (1993).
[19] E. Wakakuwa and Y. Nakata, arXiv:1903.05796 (2019).
[20] S. L. Braunstein, S. Pirandola, and K. Życzkowski, Phys. Rev. Lett. **110**, 101301 (2013).
[21] A. Almheiri, D. Marolf, J. Polchinski, and J. Sully, J. High Energy Phys. 02 (2013) 062.
[22] F. Ding and X. Hu, arXiv:1909.11256 (2019).
[23] J. Watrous, *The Theory of Quantum Information* (Cambridge University, Cambridge, England, 2018).