Unbreakable and breakable quantum censorship

Julien Pinske ●* and Jan Sperling ●

Paderborn University, Institute for Photonic Quantum Systems (PhoQS), Theoretical Quantum Science,
Warburger Straße 100, 33098 Paderborn, Germany

A protocol for regulating the distribution of quantum information between multiple parties is put forward. To prohibit the unrestricted distribution of quantum-resource states in a public quantum network, agents can apply a resource-destroying map to each sender's channel. Since resource-destroying maps only exist for affine quantum resource theories, censorship of a nonaffine resource theory is established on an operationally motivated subspace of free states. This is achieved by using what we name a resource-censoring map. The protocol is applied to censoring coherence, reference frames, and entanglement. Because of the local nature of the censorship protocol, it is, in principle, possible for collaborating parties to bypass censorship. Thus, we additionally derive necessary and sufficient conditions under which the censorship protocol is unbreakable.

I. INTRODUCTION

As Shor's algorithm for the efficient factoring of prime numbers exemplified [1], quantum information can be used to break certain cryptographic schemes [2,3], being foundational for quantum [4,5] and postquantum cryptography [6]. Because of the prospects that modern information societies will one day be dealing with a quantum internet [7–10] in which quantum channels of increasing complexity connect numerous senders and receivers, establishing certain restrictions on the sharing of quantum resources becomes a subject of ever increasing interest.

To prevent the unregulated spreading of quantum resources, such as coherence and entanglement, to malicious parties in their preparation of cryptographic attacks on critical infrastructures, governmental agencies might try to establish a form of *quantum censorship*. In such a protocol, quantum information which is deemed benign crosses a network unaltered while hazardous quantum information is rendered classical (Fig. 1). A less dystopian, but an information-processing equivalent, scenario might be the censorship of a commercialized network, with a provider offering free transmission of classical information, but demanding premium fees for the sharing of quantum information.

In this work, we devise a protocol for such quantum censorship applications. The protocol is based on a network of multiple sender-receiver pairs, being controlled by some dominant, protective agency (e.g., a governmental authority, a commercial provider, etc.) that applies a resource-destroying (RD) map [11] locally to each sender. This ensures that only free states of a quantum resource theory (QRT) [12] are transmitted over the network. RD maps distinguish themselves from resource-breaking [13,14], resource-annihilating [15], and resource-erasing protocols [16,17] in that they destroy the quantum resource but do not alter free states. Moreover, RD maps are single-shot operations, thus avoiding costly procedures such as tomography, by the agency.

The issue regarding RD maps is that they are not physically implementable for all QRTs. Indeed, only affine QRTs can give rise to a linear RD map; necessary and sufficient conditions for a QRT to have a (unique) RD map were derived in Ref. [18]. Examples of affine QRTs that possess RD maps include quantum coherence [19,20], quantum thermodynamics [21,22], and quantum reference frames [23,24]. However, there do not exist linear RD maps for real-valued quantum mechanics (affine) [25,26], quantum entanglement (convex) [27–29], quantum discord (nonconvex) [30], and non-Gaussianity (convex [31] and nonconvex [32]). At first sight, this appears to set a fundamental limitation to which resources a quantum censorship can be imposed. In the case of a nonaffine QRT, we identify affine subspaces of free states on which a censorship can still be enforced. Since these subspaces are operationally motivated (while QRTs are physically motivated), we introduce the notion of a resource-censoring (RC) map being a generalization of RD maps.

Once the censorship protocol is established, the question arises if the sending parties can use nonlocal resources, such as shared entanglement, to overcome the censorship, meaning that a resource reaches the receivers. This is, in principle, possible because the agent applies RC maps locally to each sender-receiver channel. Thus, we establish necessary and sufficient constraints on when collaborating parties can break the censorship. In particular, we find that a censorship that is realized via an RD map is unbreakable. It follows that the transmission of classical information (incoherent states) and speakable information (reference frames) can be enforced perfectly by the censorship protocol. By contrast, censorship of the (nonaffine) QRT of entanglement can be overcome by using preshared entanglement between multiple senders. Finally, the effect of noise on the protocol is discussed.
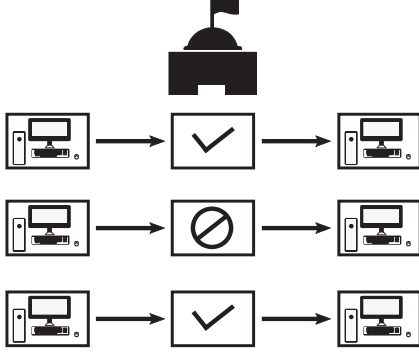
---

*julien.pinske@uni-paderborn.de

FIG. 1. In the quantum censorship protocol, a dominant, protective agency oversees quantum communication in a public-domain quantum network.

II. QUANTUM RESOURCE THEORIES

When trying to establish censorship on quantum information, we first have to split the set of quantum states into resource states, whose distribution one wants to prevent, and free states, which propagate in the network unaltered. Making this distinction is the subject of QRTs [12]. Each QRT comes with an assigned set of free states $\mathcal{F}(A)$, being a subset of the set of density operators, which we denote as $\mathcal{D}(A)$. The set $\mathcal{D}(A)$ contains positive-semidefinite, unit-trace operators ρ acting on the (here, finite-dimensional) Hilbert space $\mathcal{H}_A$ of a system A.

A QRT is said to be affine if the free states form an affine space; i.e., for any $\sigma_a \in \mathcal{F}(A)$, the state $\sigma = \sum_a t_a \sigma_a$, with $t_a \in \mathbb{R}$ and $\sum_a t_a = 1$, is again a free state. For $\mathcal{F}(A) \subseteq \mathcal{D}(A)$, its affine hull is here defined as

$$\text{Aff}(\mathcal{F}) = \left\{ \sum_a t_a \sigma_a \,\middle|\, \sigma_a \in \mathcal{F}(A), \sum_a t_a = 1 \right\} \cap \mathcal{D}(A). \quad (1)$$

Since an affine combination of states σ^a does not always yield a physical state, we made use of an intersection with the set of density operators $\mathcal{D}(A)$ in Eq. (1) such that $\text{Aff}(\mathcal{F})$ contains only physical states. For example, this could be free states that admit a quasiprobability representation [33] while resourceful states are nondecomposable; see Ref. [34] for an experiment.

Similarly, a QRT is said to be convex if the resource-free states form a convex set; i.e., for any $\sigma_a \in \mathcal{F}(A)$, the state $\sigma = \sum_a t_a \sigma_a$, with $t_a \geqslant 0$ and $\sum_a t_a = 1$, is again a free state. The convex hull of $\mathcal{F}(A) \subseteq \mathcal{D}(A)$ is

$$\text{Conv}(\mathcal{F}) = \left\{ \sum_a t_a \sigma_a \,\middle|\, \sigma_a \in \mathcal{F}(A), \sum_a t_a = 1, t_a \geqslant 0 \right\}. \quad (2)$$

Note that $\text{Conv}[\mathcal{F}(A)] \subseteq \text{Aff}[\mathcal{F}(A)]$ holds true because convex sums are a special case of affine sums where $0 \leqslant t_a \leqslant 1$ is a probability.

We denote by $\mathcal{D}(A_1, \ldots, A_N)$ the set of quantum states of an N-partite composite system. The convex hull $\text{Conv}[\mathcal{D}(A_1) \otimes \cdots \otimes \mathcal{D}(A_N)]$ corresponds to the set of N-partite, fully separable states [35,36]. Note that we here employ the following notation of tensor products of sets: $\mathcal{D}(A_1) \otimes \cdots \otimes \mathcal{D}(A_N) = \{\rho_{A_1} \otimes \cdots \otimes \rho_{A_n} | \rho_{A_1} \in \mathcal{D}(A_1), \ldots, \rho_{A_N} \in \mathcal{D}(A_N)\}$. Further, we suppose that the set

of composite free states $\mathcal{F}(A_1, \ldots, A_N)$ contains at least $\mathcal{F}(A_1) \otimes \cdots \otimes \mathcal{F}(A_N)$ [12]. This means that the independent preparation of free states by multiple parties gives a free state on the composite system. Moreover, discarding subsystems may not create a resource; i.e., for $\sigma \in \mathcal{F}(A_1, \ldots, A_N)$, its marginals $\text{Tr}_a(\sigma) \in \mathcal{F}(A_1, \ldots, A_{a-1}, A_{a+1}, \ldots, A_N)$, for $a = 1, \ldots, N$, are free as well. Therefore, if $\mathcal{F}(A_1), \ldots, \mathcal{F}(A_N)$ are affine, then one defines

$$\mathcal{F}(A_1, \ldots, A_N) = \text{Aff}[\mathcal{F}(A_1) \otimes \cdots \otimes \mathcal{F}(A_N)]. \quad (3)$$

If $\mathcal{F}(A_1), \ldots, \mathcal{F}(A_N)$ are convex, then one has

$$\mathcal{F}(A_1, \ldots, A_N) = \text{Conv}[\mathcal{F}(A_1) \otimes \cdots \otimes \mathcal{F}(A_N)]. \quad (4)$$

In addition, for a general QRT, $\mathcal{F}(A_1, \ldots, A_N) \supseteq \mathcal{F}(A_1) \otimes \cdots \otimes \mathcal{F}(A_N)$ holds true.

Resource-destroying maps and resource-censoring maps

Physical operations are mathematically expressed as quantum channels [37], i.e., linear maps $\Lambda : \mathcal{D}(A) \to \mathcal{D}(B)$ that are completely positive and trace-preserving. A quantum channel Δ is said to be RD if it additionally satisfies

(i) $\forall \rho \in \mathcal{D}(A): \quad \Delta(\rho) \in \mathcal{F}(B)$,   (resource-destroying)

(ii) $\forall \sigma \in \mathcal{F}(A): \quad \Delta(\sigma) = \sigma$.   (freeness-preserving)

In Ref. [11], it was shown that the existence of a RD map implies that $\mathcal{F}(A)$ was affine; see also Refs. [12,18]. To see this, let $\sigma = \sum_a t_a \sigma_a \notin \mathcal{F}(A)$ be an affine combination, and $\sigma_a \in \mathcal{F}(A)$ are free states. If an RD map Δ would exist for a nonaffine theory, then $\Delta(\sum_a t_a \sigma_a) = \sum_a t_a \Delta(\sigma_a)$ has to be a free state by condition (i). However, condition (ii) implies $\Delta(\sigma_a) = \sigma_a$ for all a, thus $\Delta(\sigma) = \sigma$. However, σ is not a free state by the initial assumption. Thus, we are left with a contradiction, showing that such a map Δ cannot exist.

Nevertheless, for a nonaffine QRT, a generalization of RD maps can be introduced, which we dub RC maps.

Definition 1. A channel Δ' is said to be RC if it satisfies

$$\forall \rho \in \mathcal{D}(A) : \Delta'(\rho) \in \mathcal{F}(B), \qquad \text{(resource destroying)}$$

$$\forall \sigma \in \mathcal{F}'(A) : \Delta'(\sigma) = \sigma, \qquad \text{(almost freeness-preserving)}$$

where $\mathcal{F}'(A) \subseteq \mathcal{F}(A)$ is a chosen affine subspace.
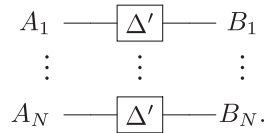
We emphasize that RC maps are not just RD maps belonging to a smaller QRT $\mathcal{F}'(A)$, with $\mathcal{F}'(A) \subseteq \mathcal{F}(A)$ since we do not demand an RC map Δ' to map any state $\rho \in \mathcal{D}(A)$ onto a state in $\mathcal{F}'(B)$. Moreover, free states $\mathcal{F}(A)$ of a QRT are commonly motivated by physical limitations while the set $\mathcal{F}'(A)$ is motivated operationally. Simply speaking, $\mathcal{F}'(A)$ is a subset of free states for which one can guarantee that these pass the channel unaltered while any resource $\rho \notin \mathcal{F}(A)$ is destroyed. The free states in $\mathcal{F}(A) \setminus \mathcal{F}'(A)$ might also undergo changes. Since $\mathcal{F}'(A_1), \ldots, \mathcal{F}'(A_N)$ are, by definition, affine, $\mathcal{F}'(A_1, \ldots, A_N)$ is given by the affine hull in Eq. (3). For an affine QRT, one has $\Delta' = \Delta$, with $\mathcal{F}'(A) = \mathcal{F}(A)$. However, for any nonaffine QRT $\mathcal{F}(A)$, one can always find at least a minimal construction $\mathcal{F}'(A) = \{\sigma\}$, containing a single state $\sigma \in \mathcal{F}(A)$; then, $\Delta'(\rho) = \text{Tr}(\rho)\sigma$ is RC.

III. QUANTUM CENSORSHIP

In the following, the quantum censorship protocol is introduced. First, the protocol is studied for noiseless channels. Second, we discuss under which circumstances multiple senders can coordinate their resources to potentially overcome censorship. After the discussion of important special cases, the effect of noise on the protocol is investigated.

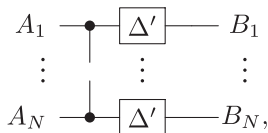### A. Censorship over noiseless channels

Consider N senders $A_1, \ldots, A_N$ who have access to local quantum resources, e.g., party A_a can prepare any state $\rho_{A_a} \in \mathcal{D}(A_a)$. In an unregulated network, each sender is connected to one of the receivers $B_1, \ldots, B_N$ via the noiseless channel $\mathrm{id}_{A_a \to B_a}$. However, to prevent the transmission of resource states, an agent sits in between each sender-receiver pair. The agent's goal is to limit the type of quantum states that can be shared between parties to the free states $\mathcal{F}(A_a)$ of a QRT. The agent informs the senders that only the transmission of free states in an affine subspace $\mathcal{F}'(A_a) \subseteq \mathcal{F}(A_a)$ is authorized, the user agreement. To enforce that policy, the agent can implement an RC map Δ'. Thus, the information processing protocol of (noiseless) quantum censorship is

$$
\begin{array}{ccc}
A_1 \ \rule[0.5ex]{1.2em}{0.4pt}\ \boxed{\Delta'}\ \rule[0.5ex]{1.2em}{0.4pt}\ & B_1 \\
\vdots & \vdots & \vdots \\
A_N \ \rule[0.5ex]{1.2em}{0.4pt}\ \boxed{\Delta'}\ \rule[0.5ex]{1.2em}{0.4pt}\ & B_N.
\end{array}
$$

As long as each sender $A_1, \ldots, A_N$ only has access to local quantum resources, i.e., the composite system is in a product state $\rho_{A_1} \otimes \cdots \otimes \rho_{A_N}$, receiving parties $B_1, \ldots, B_N$ obtain $\Delta'(\rho_{A_1}) \otimes \cdots \otimes \Delta'(\rho_{A_N})$, which is a free state in $\mathcal{F}(B_1 \ldots B_N)$, as intended by the agent. If, however, an initial state $\sigma_{A_1} \otimes \cdots \otimes \sigma_{A_N}$ belongs to $\mathcal{F}'(A_1) \otimes \cdots \otimes \mathcal{F}'(A_N)$, it remains unchanged by the action of $(\Delta')^{\otimes N}$. This allows the users of the network to carry out (undisturbed) communication only with messages $\sigma \in \mathcal{F}'(A_1, \ldots, A_N)$.

B. Breakable and unbreakable censorship

Clearly, a single sender cannot break censorship as $\rho \in \mathcal{D}(A)$ is mapped onto a free state $\Delta'(\rho) \in \mathcal{F}(B)$. But sending parties $A_1, \ldots, A_N$ might coordinate their actions to prepare a nonlocal resource state $\rho \in \mathcal{D}(A_1, \ldots, A_N)$. In this case, the circuit is

$$
\begin{array}{ccc}
A_1 \ \bullet\!\!\rule[0.5ex]{0.8em}{0.4pt}\ \boxed{\Delta'}\ \rule[0.5ex]{0.8em}{0.4pt}\ & B_1 \\
\vdots & \vdots & \vdots \\
A_N \ \bullet\!\!\rule[0.5ex]{0.8em}{0.4pt}\ \boxed{\Delta'}\ \rule[0.5ex]{0.8em}{0.4pt}\ & B_N,
\end{array}
$$

where the vertical line between the senders indicates preshared entanglement (and randomness [12]) necessary to prepare an arbitrary N-partite quantum state. Because of the local action of the agent's operation Δ', the question arises if the censorship can be overcome in this manner. Formally, we define the notion of breakable censorship as follows.

Definition 2. A censorship is breakable if there exists a state $\rho \notin \mathcal{F}(A_1, \ldots, A_N)$ such that $(\Delta')^{\otimes N}(\rho) = \rho$. Otherwise, censorship is said to be unbreakable.

Simply speaking, censorship is breakable if a quantum correlated resource state reaches the receivers unaltered. The receivers can coordinate their actions to make use of the resource.

When censorship is unbreakable, malicious users $A_1, \ldots, A_N$ cannot proliferate quantum resources, thus making it easier to attribute the origin of a cryptographic attack in places, wherever postquantum cryptography is not at its state-of-the-art. In a commercial setting, where a provider demands premium fees for sharing quantum resources, overcoming the censorship creates a free-rider problem, in which users can transmit quantum information without paying. This, in turn, destroys a provider's incentive to participate in the build-up of a global quantum internet.

The following theorem establishes for which QRTs the censorship can be overcome.

Theorem 1. A censorship is breakable, if and only if $\mathcal{F}'(A_1, \ldots, A_N) \setminus \mathcal{F}(A_1, \ldots, A_N)$ is nonempty.

Proof. If $\mathcal{F}'(A_1, \ldots, A_N) \setminus \mathcal{F}(A_1 \ldots, , A_N)$ is nonempty, then there exists a resource state $\rho \notin \mathcal{F}(A_1, \ldots, A_N)$ that is stabilized by $(\Delta')^{\otimes N}$, i.e., $(\Delta')^{\otimes N}(\rho) = \rho$. This follows from the linearity of Δ' and the definition of the affine hull $\mathcal{F}'(A_1, \ldots, A_N)$; see Eq. (3). Hence, $(\Delta')^{\otimes N}(\rho) = \rho \notin \mathcal{F}(B_1, \ldots, B_N)$ and censorship is breakable. Conversely, if censorship is breakable, then there exists a state $\rho \notin \mathcal{F}(A_1, \ldots, A_N)$ such that $(\Delta')^{\otimes N}(\rho) = \rho$. By the above argument, ρ lies in $\mathcal{F}'(A_1, \ldots, A_N) \setminus \mathcal{F}(A_1, \ldots, A_N)$, completing the proof. ∎

Intuitively, this breaking of the censorship can be understood as follows. The subset $\mathcal{F}'(A)$ of the free states $\mathcal{F}(A)$ was motivated operationally as a space on which one could establish a censorship for a single sender-receiver pair. However, its affine hull $\mathcal{F}'(A_1, \ldots, A_N)$ as defined in Eq. (3) might contain states that are resourceful on the composite system.

C. Special cases

For the case $\Delta' = \Delta$, being the (unique [18]) RD map of a QRT, we have the following theorem.

Theorem 2. Let Δ be the RD map of a QRT. Then, the censorship is unbreakable.

Proof. Since Δ is RD, the set of free states $\mathcal{F}(A)$ is affine. Hence, $\mathcal{F}(A_1, \ldots, A_N) = \mathcal{F}'(A_1 \ldots, , A_N)$, and by virtue of Theorem 1, the censorship is unbreakable. ∎

In principle, the censorship protocol can be made unbreakable for any QRT. This can be achieved by choosing $\mathcal{F}'(A) = \{\sigma\}$ as a single-state edge case. The RC map of the theory is the replacement channel $\Delta'(\rho) = \mathrm{Tr}(\rho)\sigma$. Then, $\mathcal{F}'(A_1, \ldots, A_N) = \mathcal{F}'(A_1) \otimes \cdots \otimes \mathcal{F}'(A_N)$, which is always contained in $\mathcal{F}(A_1, \ldots, A_N)$. It follows from Theorem 1 that censorship is unbreakable.

Next, suppose we are concerned with the censorship of a convex QRT. The set $\mathcal{F}(A_1, \ldots, A_N)$ as defined by the convex hull in Eq. (4) contains free, N-partite separable states. Thus, entanglement-breaking channels play a distinct role in the censorship of these resources. The channel Δ' is entanglement breaking [13] if $\mathrm{id}_{A_1 \to B_1} \otimes \Delta'$ maps any bipartite state ρ onto a separable state; i.e., $(\mathrm{id}_{A_1 \to B_1} \otimes \Delta')(\rho)$ is an element of $\mathrm{Conv}[\mathcal{D}(B_1) \otimes \mathcal{D}(B_2)]$. As Δ' is additionally RC, $\mathrm{id}_{A_1 \to B_1} \otimes \Delta'$ is a projection onto $\mathrm{Conv}[\mathcal{D}(B_1) \otimes \mathcal{F}'(B_2)]$. For

an entanglement-breaking RC map, the following theorem holds true.

Theorem 3. If Δ' is an entanglement-breaking RC map of a convex QRT, then censorship is unbreakable.

Proof. Let Δ' be entanglement breaking. Then, $(\Delta')^{\otimes N}$ is a mapping from $\mathcal{D}(A_1, \ldots, A_N)$ to the set $\mathrm{Conv}[\mathcal{F}'(B_1) \otimes \cdots \otimes \mathcal{F}'(B_N)]$. However, since $(\Delta')^{\otimes N}$ stabilizes states in the affine hull $\mathcal{F}'(A_1, \ldots, A_N)$ given by Eq. (3), it follows that
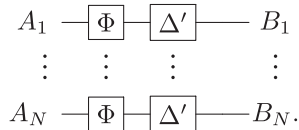
$$\mathcal{F}'(A_1, \ldots, A_N) \subseteq \mathrm{Conv}[\mathcal{F}'(A_1) \otimes \cdots \otimes \mathcal{F}'(A_N)]$$
$$\subseteq \mathcal{F}(A_1, \ldots, A_N), \tag{5}$$

where the second line follows from $\mathcal{F}'(A) \subseteq \mathcal{F}(A)$, and because $\mathcal{F}(A_1, \ldots, A_N)$ is defined via the convex hull in Eq. (4). Hence, $\mathcal{F}'(A_1, \ldots, A_N) \setminus \mathcal{F}(A_1, \ldots, A_N)$ is empty and Theorem 1 implies unbreakable censorship. ∎

For the purpose of illustration, we can make use of the minimal construction $\mathcal{F}'(A) = \{\sigma\}$ in which σ is a single free state belonging to a convex QRT $\mathcal{F}(A)$. An RC map is given by the replacement channel $\Delta'(\rho) = \mathrm{Tr}(\rho)\sigma$. Since Δ' is entanglement breaking, Theorem 3 ensures that the censorship is unbreakable, which might also be obvious from the form of the channel Δ'.

D. Censorship via noisy channels

So far, we restricted ourselves to perfect communication; that is, each sender is connected to a receiver via an identity channel. In realistic communication scenarios, however, we expect information transmission to be performed over a noisy channel $\Phi : \mathcal{D}(A_a) \to \mathcal{D}(A_a)$. While this is a well-known issue for any information processing task, in the context of the censorship protocol, we ought to be worried that the RC map Δ' introduces additional errors. Thus, we consider the noisy process Φ to occur before the operation Δ'. The protocol for the noisy case reads

$$
\begin{array}{ccccc}
A_1 & -\boxed{\Phi}- & \boxed{\Delta'} & - & B_1 \\
\vdots & \vdots & \vdots & & \vdots \\
A_N & -\boxed{\Phi}- & \boxed{\Delta'} & - & B_N.
\end{array}
$$

Throughout, it is assumed that Φ is resource nongenerating [11,12]; that is, for any free state $\sigma \in \mathcal{F}(A_a)$, one has $\Phi(\sigma) \in \mathcal{F}(A_a)$. This seems to be a reasonable assumption because we rarely expect a noisy map Φ to create a resource from a free state. If censorship is established via a RD map $\Delta' = \Delta$, then $\Delta(\sigma) = \sigma$ for any $\sigma \in \mathcal{F}(A)$. This implies that the noise Φ commutes with Δ on the set of free states, i.e.,

$$\forall \sigma \in \mathcal{F}(A): (\Delta \circ \Phi)(\sigma) = (\Phi \circ \Delta)(\sigma). \tag{6}$$

In this scenario, the censorship protocol does not introduce additional errors through the RD map Δ. This means that if a sender transmits only free states (as the agent wants them to do), their message σ is obtained by the receiver as $\Phi(\sigma)$. Of course, noiseless communication is infeasible in real-world settings, but the agent (e.g., a network provider) can aim at high-fidelity communication, avoiding the introduction of additional noise by enforcing censorship via Δ.

The situation is more delicate if we consider censorship using a RC map Δ'. The RC map stabilizes only an affine

subspace $\mathcal{F}'(A) \subseteq \mathcal{F}(A)$. States in $\mathcal{F}(A) \setminus \mathcal{F}'(A)$ could be altered by Δ'. Then, any resource-non-generating Φ that takes elements in $\mathcal{F}'(A)$ to elements in $\mathcal{F}(A) \setminus \mathcal{F}'(A)$ does not generate a resource, but it might lead Δ' to alter these states. The protocol then introduces additional changes to the state that distort the sender-receiver experience in addition to the already present noise generated by Φ. Thus, to ensure that customers can exchange free states in $\mathcal{F}'(A)$ without interference caused by the RC map Δ', the provider must, in general, keep the sender-receiver channels free of any noise process that is not an automorphism $\Phi' : \mathcal{F}'(A) \to \mathcal{F}'(A)$.

However, due to Δ' being a projection onto $\mathcal{F}'$, there might be practical situations in which the action of Δ' has a correcting effect, i.e., $\Delta'[\Phi(\sigma)]$ is closer (with respect to some metric) to σ that the noisy message $\Phi(\sigma)$.

IV. CENSORSHIP OF SPECIFIC RESOURCES

In the following, the censorship protocol is illustrated for several resources including coherence, reference frames, and entanglement.

A. Censorship of coherence

In the QRT of coherence [20,38], one quantifies the amount of superpositions in a general mixed state with respect to a fixed orthonormal basis $\{|x\rangle\}_x$, the incoherent basis. Free (likewise, incoherent) states admit a diagonal representation in that basis, $\sigma = \sum_x p_x |x\rangle \langle x|$. This QRT is affine since, by Eqs. (1) and (2), the definitions of convex and affine hull coincide in the example under study. An RD map is given by the completely dephasing channel [11,12]

$$\Delta(\rho) = \sum_x |x\rangle \langle x| \rho |x\rangle \langle x|. \tag{7}$$

Imposing censorship on coherence using Δ means that only incoherent states (classical information) are preserved during the communication. Since Δ is RD, the censorship is unbreakable, Theorem 2. This is a positive result for any provider (agent) trying to reserve quantum communication for specific costumers, while restricting the general users of the network to classical communication only. Senders have to accept such policies as there is no way of breaking the censorship.

A physical realization of the censorship can be implemented by linear optics. The sender A prepares the coherent superposition $|\psi\rangle = \alpha_H |H\rangle + \alpha_V |V\rangle$ in their laboratory. Here, horizontal and vertical polarization $|H\rangle$ and $|V\rangle$ define the incoherent basis, with $|\alpha_H|^2 + |\alpha_V|^2 = 1$. To prevent the transmission of coherent quantum information to B, the agent simply applies a polarization filter to the state $|\psi\rangle$. This realizes a projective measurement of $|H\rangle \langle H|$ or $|V\rangle \langle V|$, depending on the filter. Since the agent conceals which measurement was performed, B's best description is given by the incoherent state $\sigma = |\alpha_H|^2 |H\rangle \langle H| + |\alpha_V|^2 |V\rangle \langle V|$.

B. Censorship of reference frames

Certain types of quantum information are, without a common reference frame, of no use to the communicating parties in a network. For instance, in the QRT of coherence, one can only decide if a given state is free or not if the incoherent

basis $\{|x\rangle\}_x$ is known. Mathematically, we describe a change of the reference frame by a unitary operator U_a, relating a sender's state ρ to a receiver's state via $U_a \rho U_a^\dagger$. However, if U_a is unknown, the description of the state is obtained by averaging over all possible values in a group $\mathcal{G} = \{U_a\}_a$, i.e., $\Delta(\rho) = \frac{1}{|\mathcal{G}|} \sum_{a=1}^{|\mathcal{G}|} U_a \rho U_a^\dagger$. The channel Δ is also known as the $\mathcal{G}$-twirling map [12]. If we consider a lack of a shared reference frame to define the free states $\mathcal{F}(A) = \{\Delta(\rho) \,|\, \rho \in \mathcal{D}(A)\}$, then Δ is a projection onto $\mathcal{F}(A)$. In particular, due to $\mathcal{F}(A)$ being affine, it is the RD map of the QRT. Thus, the censorship of reference frames in unbreakable; see Theorem 2. Note that the same conclusion cannot be reached using Theorem 3. Even though $\mathcal{F}(A)$ is affine, and thus convex, Δ is generally not entanglement breaking.

C. Censorship of entanglement

In the QRT of entanglement [12,28], the set of free states $\mathcal{F}(A)$ contains all separable bipartite states of the system A, i.e., $\mathcal{H}_A = \mathcal{X}_A \otimes \mathcal{Y}_A$. A quantum state $\sigma \in \mathcal{D}(A)$ is said to be separable if it can be written as a probabilistic mixture of pure product states [35]

$$\sigma = \sum_x p_x |\psi^x\rangle \langle\psi^x|_{\mathcal{X}_A} \otimes |\phi^x\rangle \langle\phi^x|_{\mathcal{Y}_A}, \qquad (8)$$

where $p_x \geqslant 0$ and $\sum_x p_x = 1$. Mathematically, $\mathcal{F}(A)$ is the convex hull of $\mathcal{D}(\mathcal{X}_A) \otimes \mathcal{D}(\mathcal{Y}_A)$. Since $\mathcal{F}(A)$ is convex, but not affine, there is no RD map for the theory. However, if the agent informs a sender-receiver pair to agree on a fixed orthonormal basis $\{|x\rangle\}_x$ for their subsystems $\mathcal{X}_A$ and $\mathcal{X}_B$, a censorship between them can be established. This is done on the affine subspace $\mathcal{F}'(A)$, containing classical-quantum states $\sigma = \sum_x p_x |x\rangle \langle x|_{\mathcal{X}_A} \otimes \sigma_{\mathcal{Y}_A}^x$ [39], which are diagonal with respect to $\{|x\rangle\}_x$ in $\mathcal{X}_A$, and we have arbitrary $\sigma_{\mathcal{Y}_A}^x$. To see that $\mathcal{F}'(A)$ is indeed affine, consider the affine combination $\sigma = \sum_a t_a \sigma^a$ of free states $\sigma^a = \sum_x p_{x,a} |x\rangle \langle x|_{\mathcal{X}_A} \otimes \sigma_{\mathcal{Y}_A}^{x,a}$, viz.

$$\sigma = \sum_x q_x |x\rangle \langle x|_{\mathcal{X}_A} \otimes \omega_{\mathcal{Y}_A}^x \in \mathcal{F}'(A), \qquad (9)$$

where $\omega_{\mathcal{Y}_A}^x = \sum_a t_a p_{x,a} \sigma_{\mathcal{Y}_A}^{x,a} / \sum_a t_a p_{x,a}$ and $\sum_{a,x} t_a p_{x,a} = \sum_x q_x = 1$. An RC map for entanglement is defined as

$$\Delta'(\rho) = \sum_x (|x\rangle \langle x|_{\mathcal{X}_A} \otimes \mathbb{1}_{\mathcal{Y}_A}) \rho (|x\rangle \langle x|_{\mathcal{X}_A} \otimes \mathbb{1}_{\mathcal{Y}_A}). \qquad (10)$$

Note that Δ' acts trivially on the subsystems $\mathcal{Y}_A$, i.e., $\Delta' = \Delta \otimes \mathrm{id}_{\mathcal{Y}_A \to \mathcal{Y}_B}$, with Δ being the dephasing channel, Eq. (11). The channel in Eq. (10) can be used to impose censorship on entanglement. To see this, note that Δ' takes any bipartite state $\rho \in \mathcal{D}(A)$ to a separable state in $\mathcal{F}(B)$. However, not all free states $\sigma \in \mathcal{F}(A)$ are stabilized by the map in Eq. (10), but only those in $\mathcal{F}'(A)$.

In the QRT of entanglement, $\mathcal{F}(A_1, \ldots, A_N)$ is given by the convex hull in Eq. (4). In contrast, the affine hull $\mathcal{F}'(A_1, \ldots, A_N)$, as defined in Eq. (3), contains states possessing entanglement between senders $A_1, \ldots, A_N$. It follows that $\mathcal{F}'(A_1, \ldots, A_N) \setminus \mathcal{F}(A_1, \ldots, A_N)$ is nonempty, and Theorem 1 thus implies that censorship can be broken. To see this explicitly, consider two senders A_1 and A_2 sharing the state

$$\rho_{A_1 A_2} = \sum_{x,y} p_{xy} |x\rangle \langle x|_{\mathcal{X}_{A_1}} \otimes |y\rangle \langle y|_{\mathcal{X}_{A_2}} \otimes \rho_{\mathcal{Y}_{A_1} \mathcal{Y}_{A_2}}^{xy}, \qquad (11)$$

where at least one ρ^{xy} is entangled. The protocol for this case is
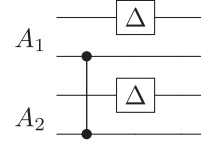
It is not hard to see that $\Delta'_{A_1} \otimes \Delta'_{A_2}$ leaves the states ρ^{xy} unaltered. Thus, entanglement is passed on to the receivers, and censorship has been broken. Note that the agent might enforce an unbreakable censorship of entanglement by resorting to a (stricter) censorship on coherence, using the RD map $\Delta^{\otimes 2}$ from Eq. (11), and redefining $\mathcal{F}'(A)$ as the set of (bipartite) incoherent states. This suffices because there cannot be entanglement without coherence, and censorship of coherence is unbreakable.

In general, the RC map in Eq. (10) does not commute with resource nongenerating (i.e., nonentangling [40,41]) noise Φ on the set of free states $\mathcal{F}(A)$. Thus, the agent must be worried that their action Δ' introduces additional errors into the message, despite a sender A using the network permissibly, i.e., sending only messages $\sigma \in \mathcal{F}'(A)$ according to the user agreement.

To illustrate the undesirable effects such noise can have on a state $\sigma = \sum_x p_x |x\rangle \langle x|_{\mathcal{X}_A} \otimes \sigma_{\mathcal{Y}_A}^x$, consider a swap channel $\Phi(\rho \otimes \sigma) = \sigma \otimes \rho$. Clearly, the noise Φ is resource nongenerating (nonentangling). After the agent, applies the RC map in Eq. (10), a receiver B is left with the incoherent state

$$(\Delta' \circ \Phi)(\sigma) = \sum_{x,y} p_x \langle y| \sigma_{\mathcal{Y}_A}^x |y\rangle |y\rangle \langle y|_{\mathcal{X}_B} \otimes |x\rangle \langle x|_{\mathcal{Y}_B}. \qquad (12)$$

This leaves B without any quantum properties left in the state. While a swap channel might be a nonintuitive form of noise, mixing up a bit sequences is certainly possible, and it highlights some of the difficulties (quantum) network providers (i.e., the agent) faces when trying to establish a quantum censorship, while still keeping the network operable.

A physical realization of the censorship can be devised using linear optics. Two senders A_1 and A_2 prepare the entangled state

$$\rho_{A_1 A_2} = |H\rangle \langle H|_{\mathcal{X}_{A_1}} \otimes |V\rangle \langle V|_{\mathcal{X}_{A_2}} \otimes |\phi^+\rangle \langle \phi^+|_{\mathcal{Y}_{A_1} \mathcal{Y}_{A_2}}.$$

Here, horizontal and vertical polarization $|H\rangle$ and $|V\rangle$ define the incoherent basis and $|\phi^+\rangle = (|HH\rangle + |VV\rangle)/\sqrt{2}$ is a Bell state. The agent tries to prevent the transmission of entanglement to receivers B_1 and B_2 using the RC map (10). There, the agent performs a (nonselective) polarization measurement on the subsystems $\mathcal{X}_{A_1}$ and $\mathcal{X}_{A_2}$, thus realizing a dephasing with respect to the states $|H\rangle$ and $|V\rangle$ [see Eq. (11)]. See also

Ref. [42] for experimental results on a controllable dephasing channel. However, the agent does not apply any operation to the subsystems $\mathcal{Y}_{A_1}$ and $\mathcal{Y}_{A_2}$ [see Eq. (10)]. It follows that the state $\rho_{A_1 A_2}$ is not altered by the RC map $\Delta'_{A_1} \otimes \Delta'_{A_2}$. The entangled state $|\phi^+\rangle \langle\phi^+|$, thus reaches the receivers B_1 and B_2. The censorship has been broken.

V. CONCLUSION

We introduced a protocol for quantum censorship. Therein, an agent can apply RC or RD maps locally to each sender-receiver connection, thus prohibiting the distribution of resource states through the network at will. By using such maps, the protocol avoids any measurements of a state, which would render the network unusable for quantum communication. Since RD maps exist only for affine QRTs, RC maps were utilized to impose censorship on an affine subspace of free states. Our necessary and sufficient conditions reveal under which censorship is unbreakable. This was the case for the QRT of coherence and reference frames while the censorship of entanglement could be overcome.

Quantum censorship protocol becomes especially urgent once we are confronted with the emergence of a widely accessible quantum internet. See, for instance, Refs. [43,44] for recent experimental progress in this direction. On the one hand, quantum censorship allows governmental authorities to prevent ill-intentioned parties from quantum-cryptographic attacks. On the other hand, commercial enterprises may offer free classical services but want to charge premium fees for quantum communication. Also, future studies of more advanced (possibly nonlocal) censorship protocols might be a worthwhile endeavor. We hope our work paves the way for a discussion of quantum censorship as a previously unappreciated tool in quantum communication.

[1] P. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Sci. Statist. Comput. **26**, 1484 (1997).

[2] V. Mavroeidis, K. Vishi, M. D. Zych, and A. Josang, The impact of quantum computing on present cryptography, Int. J. Adv. Comput. Sci. Appl. **9**, 1 (2018).

[3] M. Sharma, V. Choudhary, R. S. Bhatia, S. Malik, A. Raina, and H. Khandelwal, Leveraging the power of quantum computing for breaking RSA encryption, Cyber-Physical Systems **7**, 73 (2021).

[4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145 (2002).

[5] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Advances in quantum cryptography, Adv. Opt. Photon. **12**, 1012 (2020).

[6] D. Bernstein and T. Lange, Post-quantum cryptography, Nature (London) **549**, 188 (2017).

[7] H. Kimble, The quantum internet, Nature (London) **453**, 1023 (2008).

[8] S. Wehner, D. Elkouss, and R. Hanson, Quantum internet: A vision for the road ahead, Science **362**, eaam9288 (2018).

[9] J. Illiano, M. Caleffi, A. Manzalini, and A. S. Cacciapuoti, Quantum internet protocol stack: A comprehensive survey, Computer Networks **213**, 109092 (2022).

[10] D. Ribezzo, M. Zahidy, I. Vagniluca, N. Biagi, S. Francesconi, T. Occhipinti, L. K. Oxenløwe, M. Lončarić, I. Cvitić, M. Stipčević, Ž. Pušavec, R. Kaltenbaek, A. Ramšak, F. Cesa, G. Giorgetti, F. Scazza, A. Bassi, P. De Natale, F. S. Cataliotti, M. Inguscio *et al.*, Deploying an inter-european quantum network, Adv. Quantum Technol. **6**, 2200061 (2023).

[11] Z.-W. Liu, X. Hu, and S. Lloyd, Resource destroying maps, Phys. Rev. Lett. **118**, 060502 (2017).

[12] E. Chitambar and G. Gour, Quantum resource theories, Rev. Mod. Phys. **91**, 025001 (2019).

[13] M. Horodecki, P. W. Shor, and M. B. Ruskai, Entanglement breaking channels, Rev. Math. Phys. **15**, 629 (2003).

[14] J. S. Ivan, K. Kumar Sabapathy, and R. Simon, Nonclassicality breaking is the same as entanglement breaking for bosonic Gaussian channels, Phys. Rev. A **88**, 032302 (2013).

[15] L. Moravčíková and M. Ziman, Entanglement-annihilating and entanglement-breaking channels, J. Phys. A: Math. Theor. **43**, 275306 (2010).

[16] B. Groisman, S. Popescu, and A. Winter, Quantum, classical, and total amount of correlations in a quantum state, Phys. Rev. A **72**, 032317 (2005).

[17] U. Singh, M. N. Bera, A. Misra, and A. K. Pati, Erasing quantum coherence: An operational approach, arXiv:1506.08186.

[18] G. Gour, Quantum resource theories in the single-shot regime, Phys. Rev. A **95**, 062314 (2017).

[19] J. Aberg, Quantifying superposition, arXiv:quant-ph/0612146.

[20] T. Baumgratz, M. Cramer, and M. B. Plenio, Quantifying coherence, Phys. Rev. Lett. **113**, 140401 (2014).

[21] F. Brandão, M. Horodecki, N. Ng, J. Oppenheim, and S. Wehner, The second laws of quantum thermodynamics, Proc. Natl. Acad. Sci. USA **112**, 3275 (2015).

[22] C. Sparaciari, L. D. Rio, C. M. Scandolo, P. Faist, and J. Oppenheim, The first law of general quantum resource theories, Quantum **4**, 259 (2020).

[23] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, Reference frames, superselection rules, and quantum information, Rev. Mod. Phys. **79**, 555 (2007).

[24] G. Gour and R. W. Spekkens, The resource theory of quantum reference frames: Manipulations and monotones, New J. Phys. **10**, 033023 (2008).

[25] A. Hickey and G. Gour, Quantifying the imaginarity of quantum mechanics, J. Phys. A: Math. Theor. **51**, 414009 (2018).

[26] K.-D. Wu, T. V. Kondra, S. Rana, C. M. Scandolo, G.-Y. Xiang, C.-F. Li, G.-C. Guo, and A. Streltsov, Operational resource theory of imaginarity, Phys. Rev. Lett. **126**, 090401 (2021).

[27] J. I. Cirac, W. Dür, B. Kraus, and M. Lewenstein, Entangling operations and their implementation using a small amount of entanglement, Phys. Rev. Lett. **86**, 544 (2001).

[28] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. **81**, 865 (2009).

[29] E. Chitambar, J. I. de Vicente, M. W. Girard, and G. Gour, Entanglement manipulation beyond local operations and classical communication, J. Math. Phys. **61**, 042201 (2020).

[30] H. Ollivier and W. H. Zurek, Quantum discord: A measure of the quantumness of correlations, Phys. Rev. Lett. **88**, 017901 (2001).

[31] R. Takagi and Q. Zhuang, Convex resource theory of non-Gaussianity, Phys. Rev. A **97**, 062337 (2018).

[32] L. Lami, B. Regula, X. Wang, R. Nichols, A. Winter, and G. Adesso, Gaussian quantum resource theories, Phys. Rev. A **98**, 022335 (2018).

[33] J. Sperling and I. A. Walmsley, Quasiprobability representation of quantum coherence, Phys. Rev. A **97**, 062327 (2018).

[34] N. Prasannan, S. De, S. Barkhofen, B. Brecht, C. Silberhorn, and J. Sperling, Experimental entanglement characterization of two-rebit states, Phys. Rev. A **103**, L040402 (2021).

[35] R. F. Werner, Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model, Phys. Rev. A **40**, 4277 (1989).

[36] P. Horodecki, Separability criterion and inseparable mixed states with positive partial transposition, Phys. Lett. A **232**, 333 (1997).

[37] J. Watrous, *The Theory of Quantum Information* (Cambridge University Press, Cambridge, England, 2018).

[38] J. Sperling and W. Vogel, Convex ordering and quantification of quantumness, Phys. Scr. **90**, 074024 (2015).

[39] A. Datta, A condition for the nullity of quantum discord, arXiv:1003.5256.

[40] A. W. Harrow and M. A. Nielsen, Robustness of quantum gates in the presence of noise, Phys. Rev. A **68**, 012308 (2003).

[41] S. Virmani, S. F. Huelga, and M. B. Plenio, Classical simulability, entanglement breaking, and quantum computation thresholds, Phys. Rev. A **71**, 042328 (2005).

[42] D. F. Urrego, J.-R. Álvarez, O. Calderón-Losada, J. Svozilík, M. Nuñez, and A. Valencia, Implementation and characterization of a controllable dephasing channel based on coupling polarization and spatial degrees of freedom of light, Opt. Express **26**, 11940 (2018).

[43] S. P. Neumann, A. Buchner, L. Bulla, M. Bohmann, and R. Ursin, Continuous entanglement distribution over a transnational 248 km fiber link, Nat. Commun. **13**, 6134 (2022).

[44] H. Zhang, Z. Sun, R. Qi, L. Yin, G.-L. Long, and J. Lu, Realization of quantum secure direct communication over 100 km fiber with time-bin and phase quantum states, Light Sci. Appl. **11**, 83 (2022).