

Quantum Channel Masking

Anna Honeycutt*

*Department of Physics,
University of Illinois Urbana-Champaign, Urbana, IL, USA*

Hailey Murray†

*Department of Physics,
Embry-Riddle Aeronautical University,
Prescott, AZ, USA and
School of Applied and Engineering Physics,
Cornell University, Ithaca, NY, USA*

Eric Chitambar‡

*Department of Electrical and Computer Engineering, Coordinated Science Laboratory,
University of Illinois Urbana-Champaign, Urbana, IL, USA*

(Dated: October 13, 2025)

Quantum masking is a special type of secret sharing in which some information gets reversibly distributed into a multipartite system, leaving the original information inaccessible to each subsystem. This paper proposes a dynamical extension of quantum masking to the level of quantum channels. In channel masking, the identity of a channel becomes locally hidden but still globally accessible after its output is sent through a bipartite broadcasting channel. We first characterize all families of d -dimensional unitaries that can be isometrically masked, a condition that holds even in the presence of depolarizing noise. For the case of qubits, we identify which families of Pauli channels can be masked, and we prove that a qubit channel can be masked with the identity if and only if it is unital and has a pure-state fixed point. Masking with the identity describes a scenario in which channel noise becomes completely delocalized through a broadcast map and undetectable through subsystem dynamics alone.

There are several no-go theorems of great importance to quantum information processing, such as the no-cloning [1] and the no-broadcasting theorems [2, 3]. Additionally, the no-deleting theorem states that we cannot delete unknown quantum information in a closed system [4], and due to the no-hiding theorem, quantum information that is lost in one subsystem of a closed composite system must be recoverable from the other subsystem [5]. These no-go theorems have had significant applications in error correction [6], quantum key distribution [7] and secret sharing [8, 9].

As a modification to the original problem of hiding quantum information [5], Modi et. al. proposed the task of quantum masking [10]. This involves reversibly splitting states from a given set into two parts such that the identity of the original state cannot be determined by examining either of the parts individually (see Fig. 1). While the no-hiding theorem implies this is impossible for arbitrary states drawn from a Hilbert space with a pure ancilla system, it was shown that masking is possible for restricted sets of states [10]. In fact, maskable sets of states can be much richer than cloneable sets, the latter consisting of just orthonormal pure states. For qubits, any set of states whose Bloch vectors fall on a single disk

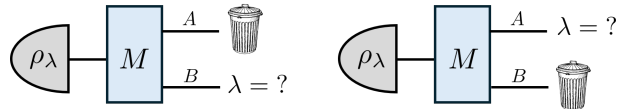


FIG. 1. In state masking, a set of states $\mathcal{S} = \{\rho_\lambda\}_\lambda$ is masked by the isometry M such that the reduced state outputs are independent of λ . Here, the trash can is used to represent a discarding of the subsystem, which mathematically corresponds to a partial trace.

in the Bloch sphere can be masked [11, 12], and a similar geometrical structure appears to hold for the sets of higher-dimensional maskable states [12]. Additionally, it has been shown that all qubit states can be masked if we move beyond bipartite splitting and consider multipartite masking [13]. This, in fact, is a direct consequence of the fact that every quantum error correcting code accomplishes the task of quantum masking, and connections between the two have been studied [13, 14]. In particular, multipartite masking enables the possibility of quantum secret sharing [8, 9, 15], where quantum information is distributed among several parties such that the original information is inaccessible without collaboration. Masking also has applications in other cryptographic tasks such as quantum bit commitment [10, 16].

Here, we propose an extension of quantum masking to sets of quantum channels or quantum gates. As depicted in Fig. 2, this is a generalization of state mask-

* annagh2@illinois.edu

† hm649@cornell.edu

‡ echitamb@illinois.edu

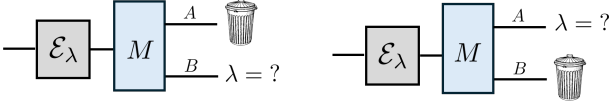


FIG. 2. In channel masking, a set of channels or gates $\mathcal{S} = \{\mathcal{E}_\lambda\}_\lambda$ is masked by the isometry M such that the reduced channels are independent of λ .

ing in which some reversible splitting is performed as post-processing to a random channel quantum $\mathcal{E}_\lambda$ chosen from some set $\mathcal{S} = \{\mathcal{E}_\lambda\}_\lambda$. The masking is successful if the two reduced channels are independent of λ , thereby hiding the “which channel” information from local recovery; only by examining the global channel $\mathcal{U}_M \circ \mathcal{E}_\lambda(\cdot) \equiv M[\mathcal{E}(\cdot)]M^\dagger$ can the value λ be perfectly recovered. This problem is similar in spirit but conceptually distinct from the well-studied task of hiding the “which channel” information of a state-dependent channel between a sender and one receiver [17–19]. In that scenario, one attempts to minimize the leakage rate of the state parameter λ through channel encoding. In contrast, the problem considered here involves a single shot use of the channel or gate, and the parameter λ gets masked in the bipartite correlations generated after the channel or gate.

A special case of this problem considers masking just a single noisy channel $\mathcal{E}$ from the ideal identity channel, id . In this scenario, the masker serves as a broadcasting map $M : \mathcal{H}_Q \rightarrow \mathcal{H}_{AB}$ that completely hides the effect of $\mathcal{E}$ from the subsystems A and B , i.e.

$$\text{Tr}_X[M\rho M^\dagger] = \text{Tr}_X[M\mathcal{E}(\rho)M^\dagger], \quad X \in \{A, B\}, \quad \forall \rho. \quad (1)$$

Since the broadcasting can be inverted, the information of whether or not the noisy map is present must be accessible somewhere in the overall system, and in this case, that information lies entirely in the correlations between subsystems A and B .

In this work, we focus on the masking of qubit channels and sets of qudit (unitary) gates. As one of our main results, we derive necessary and sufficient conditions for when an arbitrary number of qudit gates can be masked, and we provide an explicit construction of a masker. For qubit gates, these conditions admit an appealing geometrical interpretation on the Bloch sphere. We then focus on the masking of qubit channels and characterize all the families of noisy Pauli channels that can be masked. We further identify all qubit channels whose action can be masked with the identity (i.e. satisfy Eq. (1)). Finally, we consider the masking of classical channels. While classical Boolean circuits are unable to mask families of classical channels, we observe that conjugate coding provides a natural construction of a quantum masker of arbitrary classical channels. Before presenting our results, we provide a more precise statement of our problem and an overview of definitions. We then proceed to our main results and conclude the paper with a brief discussion on future directions of work.

I. PRELIMINARIES

We begin by defining the notion of state masking presented in Ref. [10]. Let $M : \mathcal{H}_Q \rightarrow \mathcal{H}_{AB}$ be an isometric mapping (meaning $M^\dagger M = \mathbb{1}_Q$) from system Q into a bipartite system AB . The map is said to mask quantum information contained in the set of states $\mathcal{S} = \{|\psi_\lambda\rangle\}_\lambda \subset \mathcal{H}_Q$ if the states $\{|\Psi_\lambda\rangle_{AB} := M|\psi_\lambda\rangle_Q\}_\lambda$ have the same marginal states, i.e.

$$\rho_A = \text{Tr}_B|\Psi_\lambda\rangle\langle\Psi_\lambda|, \quad \rho_B = \text{Tr}_A|\Psi_\lambda\rangle\langle\Psi_\lambda| \quad (2)$$

for all λ . By definition the marginal states contain no information on the original input state. However, the choice of isometric mapping M allows for the recovery of this information.

We remark that the definition of state masking presented here follows current literature and restricts M to be an isometric mapping [10–13]. Of course, one could also consider maskers $\mathcal{M}$ that are more general completely-positive trace-preserving (CPTP) maps. However, this more general model of masking allows for the potential of eavesdroppers and dishonest parties. For example, the full set of qubit states gets masked under the mapping $|\psi\rangle\langle\psi| \mapsto \mathcal{M}(|\psi\rangle\langle\psi|) = \frac{1}{4} \sum_{m,n} (X^m Z^n |\psi\rangle\langle\psi| Z^n X^m)_A \otimes |mn\rangle\langle mn|_B$, where X and Z are Pauli operators; one can directly verify that both $\text{Tr}_A \mathcal{M}(|\psi\rangle\langle\psi|)$ and $\text{Tr}_B \mathcal{M}(|\psi\rangle\langle\psi|)$ are completely mixed for every $|\psi\rangle$. Yet, in a purified picture, up to a basis change on E the map $\mathcal{M}$ arises from some dilation $U_{Q \rightarrow ABE} = \sum_{m,n} X^m Z^n \otimes |mn\rangle\langle mn|_B \otimes |mn\rangle\langle mn|_E$ such that $\mathcal{M}(\rho) = \text{Tr}_E(U\rho U^\dagger)$. If Alice were to have access to system E , then she could correct the Pauli $Z^n X^m$ on her system and perfectly obtain the state $|\psi\rangle$. One might then be motivated to demand the strongest form of masking and require that Alice has no information about the input state even if she had access to any additional side information outside of Bob’s system, meaning that the output of the masker should be a bipartite pure state. Such is the attitude taken in traditional studies of quantum key distribution (QKD) [20], and it is one we likewise adopt here. Thus, throughout this work we will assume that all maskers are isometric in form.

The task of bipartite state masking has been completely characterized in the qubit setting [11, 12], as initially conjectured in Ref. [10]. Specifically, a set of maskable qubit states corresponds to a two-dimensional hyperdisk on the Bloch sphere [12]. A similar geometric structure is suggested to persist in higher dimensions, as evidenced in the case of qutrits [12], though a complete characterization of d -dimensional masking remains to be studied. While universal bipartite masking of arbitrary states is impossible [10], it has been shown that universal multipartite masking is possible: all states in $\mathcal{C}^d$ may be masked by a multipartite masker with the addition of $2d - 1$ systems of dimension d [13].

We now extend the concept of state masking to quantum channels. A quantum channel $\mathcal{E}$ is defined as

a CPTP map from input system Q to output system Q' , and the collection of all such maps we denote as $\text{CPTP}(Q \rightarrow Q')$. We say that a set of channels $\mathcal{S} = \{\mathcal{E}_\lambda\}_\lambda \subset \text{CPTP}(Q \rightarrow Q')$ is maskable if there exists an isometry $M : \mathcal{H}_{Q'} \rightarrow \mathcal{H}_{AB}$ such that

$$\alpha(\cdot) = \text{Tr}_B[M\mathcal{E}_\lambda(\cdot)M^\dagger], \quad \beta(\cdot) = \text{Tr}_A[M\mathcal{E}_\lambda(\cdot)M^\dagger], \quad (3)$$

where $\alpha(\cdot)$ and $\beta(\cdot)$ are fixed channels independent of λ . The latter conditions mean that the identity of the applied channel $\mathcal{E}_\lambda$ is hidden from each subsystem, while still being globally recoverable via the isometry M (see Fig. 2). A special instance of this problem involves families of unitary gates $\{U_\lambda\}_\lambda$, and we say that a set of gates can be masked if the corresponding set of channels $\{\mathcal{U}_\lambda\}_\lambda$ can be masked, where $\mathcal{U}_\lambda(\cdot) := U_\lambda(\cdot)U_\lambda^\dagger$.

A useful observation is that applying pre- and post-unitaries to a family of channels does not alter its ability to be masked. That is, the channels $\{\mathcal{E}_\lambda\}_\lambda$ can be masked iff $\{\mathcal{U}_{\text{post}} \circ \mathcal{E}_\lambda \circ \mathcal{U}_{\text{pre}}\}_\lambda$ can be masked for any choice of unitaries U_{pre} and U_{post} independent of λ , a fact that can be directly verified from the definition in Eq. (3). These unitary degrees of freedom will be used heavily when studying the masking of qubit channels below.

II. RESULTS

A. Masking families of unitaries

We now present our findings on the problem of channel masking. We begin by restricting our attention to the masking of unitary gates $\{U_\lambda\}_\lambda$ that act on some d -dimensional quantum system $\mathcal{H}_Q \cong \mathbb{C}^d$. The following structural lemma pertains to the masking of a single unitary U and the identity $\mathbb{1}$.

Proposition 1. *Suppose that $M : \mathcal{H}_Q \rightarrow \mathcal{H}_{AB}$ is a masker for the two unitaries $\{\mathbb{1}, U\}$. Let $|e_1\rangle$ and $|e_2\rangle$ be any two eigenstates of U belonging to distinct eigenspaces. Then M must map $|e_1\rangle$ and $|e_2\rangle$ to locally orthogonal states. In other words,*

$$\text{Tr}_X(M|e_1\rangle\langle e_1|M^\dagger) \perp \text{Tr}_X(M|e_2\rangle\langle e_2|M^\dagger) \quad (4)$$

for $X \in \{A, B\}$, where $\perp$ denotes operators with orthogonal supports.

In the language of [21], the masker M must “broadcast the orthogonality” of the eigenstates $|e_1\rangle$ and $|e_2\rangle$.

Proof. Consider an arbitrary superposition $|\psi\rangle = \cos\theta|e_1\rangle + \sin\theta e^{i\phi}|e_2\rangle$ such that $U|\psi\rangle = \cos\theta\lambda_1|e_1\rangle + \sin\theta e^{i\phi}\lambda_2|e_2\rangle$, where λ_1 and λ_2 are the distinct eigenvalues of U for eigenstates $|e_1\rangle$ and $|e_2\rangle$. Write $|E_i\rangle_{AB} =$

$M|e_i\rangle$. Then since $|\lambda_1|^2 = |\lambda_2|^2 = 1$, we have

$$\begin{aligned} \text{Tr}_X(M|\psi\rangle\langle\psi|M^\dagger) &= \cos^2\theta \text{Tr}_X|E_1\rangle\langle E_1| + \sin^2\theta \text{Tr}_X|E_2\rangle\langle E_2| \\ &\quad + \cos\theta \sin\theta (e^{-i\phi} \text{Tr}_X|E_1\rangle\langle E_2| + \text{h.c.}) \\ \text{Tr}_X(MU|\psi\rangle\langle\psi|U^\dagger M^\dagger) &= \cos^2\theta \text{Tr}_X|E_1\rangle\langle E_1| + \sin^2\theta \text{Tr}_X|E_2\rangle\langle E_2| \\ &\quad + \cos\theta \sin\theta (e^{-i\phi} \lambda_1 \lambda_2^* \text{Tr}_X|E_1\rangle\langle E_2| + \text{h.c.}). \end{aligned}$$

Since M is a masker, the partial trace of both density matrices must be equal, which means that

$$e^{-i\phi}(1 - \lambda_1 \lambda_2^*) \text{Tr}_X|E_1\rangle\langle E_2| + \text{h.c.} = 0.$$

Note that $(1 - \lambda_1 \lambda_2^*) \neq 0$ since $\lambda_1 \neq \lambda_2$. For this to hold for any choice of ϕ , we must have that

$$\text{Tr}_X|E_1\rangle\langle E_2| = \text{Tr}_X|E_2\rangle\langle E_1| = 0. \quad (5)$$

Let $|E_1\rangle = \sum_{i=1}^d |i\rangle_A |\varphi_i\rangle_B$ and $|E_2\rangle = \sum_{i=1}^d |i\rangle_A |\varphi'_i\rangle_B$ so that

$$0 = \text{Tr}_B|E_1\rangle\langle E_2| = \sum_{i,j=1}^d |i\rangle\langle j| \langle \varphi'_j | \varphi_i \rangle,$$

which requires that $\langle \varphi'_j | \varphi_i \rangle = 0$ for all i, j . Therefore,

$$\text{Tr}_A|E_1\rangle\langle E_1| \text{Tr}_A|E_2\rangle\langle E_2| = \sum_{i,j=1}^d |\varphi_i\rangle\langle\varphi_i| |\varphi'_j\rangle\langle\varphi'_j| = 0.$$

This establishes the orthogonality of $\text{Tr}_A(M|e_1\rangle\langle e_1|M^\dagger)$ and $\text{Tr}_A(M|e_2\rangle\langle e_2|M^\dagger)$. A similar argument shows orthogonality for Alice’s reduced states. It is interesting to note that Eq. (5), the key step in this proof, also appears in the no-go state masking proof of Ref. [10]. $\square$

We now use Proposition 1 to prove our first main result, which is a full characterization of maskable gate sets.

Theorem 1. *A set of N unitary gates $\{U_n\}_{n=1}^N$ on $\mathbb{C}^d$ can be masked iff $\{U_1^\dagger U_n\}_{n=2}^N$ forms a pairwise commuting set.*

Remark 1. Multiplying by $U_1^\dagger$ in this theorem is arbitrary since the set $\{U_1^\dagger U_n\}_{n=2}^N$ is pairwise commuting iff $\{U_k^\dagger U_n\}_{n=2}^N$ is pairwise commuting for any other U_k in the set. Indeed, the commuting relations $[U_1^\dagger U_m, U_1^\dagger U_n] = 0$ for any m, n implies the equalities

$$\begin{cases} U_n^\dagger U_m = U_1^\dagger U_m U_n^\dagger U_1 \\ U_n^\dagger U_k = U_1^\dagger U_k U_n^\dagger U_1 \\ U_k^\dagger U_m = U_1^\dagger U_m U_k^\dagger U_1 \end{cases}.$$

Multiplying the second and third together and comparing with the first shows that $U_m U_n^\dagger = U_k U_n^\dagger U_m U_k^\dagger$, which says that $[U_k^\dagger U_m, U_k^\dagger U_n] = 0$.

We now turn to the proof of Theorem 1.

Proof. Let $\{U_n\}_{n=1}^N$ be an arbitrary set of unitaries on $\mathbb{C}^d$. By the observation made after Eq. (3) above, this is maskable iff the set $\{\mathbb{1}, W_n\}_{n=2}^N$ is also maskable, where $W_n := U_1^\dagger U_n$. Therefore, the proof of Theorem 1 amounts to showing that the set $\{\mathbb{1}, W_n\}_{n=2}^N$ can be masked iff the W_n are pairwise commuting.

($\Leftarrow$) Let $\{\mathbb{1}, W_n\}_{n=2}^N$ be a full set of pairwise commuting elements, and let $\{|f_k\rangle\}_{k=1}^d$ be a common orthonormal eigenbasis. Then consider a bipartite masker $M : \mathbb{C}^d \rightarrow \mathbb{C}^d \otimes \mathbb{C}^d$ of the form $M = \sum_{k=1}^d |kk\rangle \langle f_k|$. For an arbitrary state $|\psi\rangle = \sum_{k=1}^d \alpha_k |f_k\rangle \in \mathbb{C}^d$. Any unitary in $\{\mathbb{1}, W_n\}_{n=2}^N$ will act as $|\psi\rangle \mapsto |\psi'\rangle = \sum_{k=1}^d \alpha_k e^{i\phi_k} |f_k\rangle$ for some phases ϕ_k . The masker then transforms

$$M|\psi'\rangle = \sum_{k=1}^d \alpha_k e^{i\phi_k} |kk\rangle,$$

whose reduced states are completely independent of the phases ϕ_k due to the orthonormality of the $|k\rangle$. Hence the action of the arbitrary unitary in $\{\mathbb{1}, W_n\}_{n=2}^N$ has been masked.

($\Rightarrow$) Suppose that a masker M exists for the set $\{\mathbb{1}, W_n\}_{n=2}^N$. We want to show that this is a pairwise commuting set. An arbitrary pair $U, V \in \{W_n\}_{n=2}^N$ will commute with each other iff for every eigenvector $|e\rangle$ of U , the state $V|e\rangle$ is also an eigenvector of U with the same eigenvalue as $|e\rangle$. Now suppose on the contrary that $[U, V] \neq 0$. Then U has some eigenvector $|e\rangle$ such that $V|e\rangle$ does not belong to same eigenspace as $|e\rangle$. This means there exists some other eigenvector $|e'\rangle$ of U in a different eigenspace than $|e\rangle$ such that

$$0 \neq \langle e'|V|e\rangle = \langle e'|M^\dagger M V|e\rangle. \quad (6)$$

Since M is a masker for the set $\{\mathbb{1}, V\}$, the bipartite states $MV|e\rangle$ and $M|e\rangle =: |E\rangle$ must purify the same reduced density matrices. Hence, there exists a unitary T such that $MV|e\rangle = \mathbb{1} \otimes T|E\rangle$. Denoting $|E'\rangle = M|e'\rangle$, the previous equation can be written as

$$0 \neq \langle E'|\mathbb{1} \otimes T|E\rangle. \quad (7)$$

However, since M also masks $\{\mathbb{1}, U\}$, Proposition 1 requires that $\text{Tr}_B|E'\rangle\langle E'| \perp \text{Tr}_B|E\rangle\langle E|$, which would imply that $\langle E'|\mathbb{1} \otimes T|E\rangle = 0$. From this contradiction, we conclude that $[U, V] = 0$, which means the set $\{\mathbb{1}, W_n\}_{n=2}^N$ is pairwise commuting. $\square$

Remark 2. Recall that every qubit pure state can be represented by a unit vector $\hat{n}$ on the surface of the unit sphere in $\mathbb{R}^3$, and unitary gates $U \in SU(2)$ correspond to three-dimensional rotations $O \in SO(3)$. For qubit systems, an alternative and illustrative proof for the converse of Theorem 1 can be given in terms of this Bloch sphere geometry. Consider two states $|r\rangle, |r'\rangle$ that lie on the disk in $\mathbb{R}^3$ perpendicular to the Bloch sphere axis of

rotation $\hat{n}_r$ of W_1 , and define $W_1|r\rangle = |r'\rangle$. Denote the plane containing this disk by $\mathcal{P}$. Let W_2 map $|r\rangle, |r'\rangle$ to states $|s\rangle, |s'\rangle$ so that we have

$$W_1|r\rangle = |r'\rangle, \quad W_2|r\rangle = |s\rangle, \quad W_2|r'\rangle = |s'\rangle. \quad (8)$$

If there exists a masker M for $\{\mathbb{1}, W_1, W_2\}$, then it must mask the set of states $\{|r\rangle, |r'\rangle, |s\rangle\}$, corresponding to the set of unitaries $\{\mathbb{1}, W_1, W_2\}$ acting on $|r\rangle$. Thus, $\text{Tr}_B[M|\psi\rangle\langle\psi|M^\dagger]$ must be constant for all $|\psi\rangle \in \{|r\rangle, |r'\rangle, |s\rangle\}$. On the other hand, M must also mask the set of states $\{|r'\rangle, |s'\rangle\}$, corresponding to $\{\mathbb{1}, W_2\}$ acting on $|r'\rangle$, which means that $\text{Tr}_B[M|\phi\rangle\langle\phi|M^\dagger]$ must also be constant for all $|\phi\rangle \in \{|r'\rangle, |s'\rangle\}$. Since $|r'\rangle$ is common to both sets $\{|r\rangle, |r'\rangle, |s\rangle\}$ and $\{|r'\rangle, |s'\rangle\}$, the reduced density matrices must be constant when M acts on all the $\{|r\rangle, |r'\rangle, |s\rangle, |s'\rangle\}$, i.e. M masks this entire set of states. However, it is known that this is possible iff the states lie on a single hyperdisk on the Bloch sphere [12], thus the set $\{|r\rangle, |r'\rangle, |s\rangle, |s'\rangle\}$ must all lie within the plane $\mathcal{P}$. By definition, W_1 is a rotation about the axis $\hat{n}_r$ perpendicular to $\mathcal{P}$. By Eq. (8), W_2 maps an arbitrary state $|v\rangle = a|r\rangle + b|r'\rangle \in \mathcal{P}$ to state $W_2|v\rangle = a|s\rangle + b|s'\rangle \in \mathcal{P}$. Then we have $W_2(\mathcal{P}) = \mathcal{P}$, i.e. the plane $\mathcal{P}$ is preserved under the rotation W_2 . Therefore, the axis of rotation of W_2 must be $\hat{n}_r$, and so W_1 and W_2 share an axis of rotation and must commute.

Example 1. Consider the set of unitary operators composed of Pauli-X and Z gates $\{X, XZ, X\sqrt{Z}\}$. Note that this is not a pairwise commuting set, however multiplying by $X^\dagger$ we consider the transformed set $\{\mathbb{1}, Z, \sqrt{Z}\}$. Now fully pairwise commuting, this set is maskable by Theorem 1, and thus the original set $\{X, XZ, X\sqrt{Z}\}$ is maskable. A masker M may then be constructed by the common eigenvectors of $\{\mathbb{1}, Z, \sqrt{Z}\}$, where the masker for the original isometry is defined by $MX^\dagger$.

B. Masking noisy qubit channels

We now move beyond the masking of gates and consider noisy channels. Perhaps the simplest generalization involves mixing unitary gates with depolarizing noise. These are families of channels $\{\mathcal{E}_{U_\lambda}^{(p)}\}_\lambda$ where

$$\mathcal{E}_{U_\lambda}^{(p)}(\cdot) = pU_\lambda(\cdot)U_\lambda^\dagger + (1-p)\frac{\mathbb{1}}{d} \quad (9)$$

with fixed p and varying U_λ . One sees that the $\{\mathcal{E}_{U_\lambda}^{(p)}\}_\lambda$ can be masked by masker M iff for $X \in \{A, B\}$

$$p\text{Tr}_X[MU_\lambda(\cdot)U_\lambda^\dagger M^\dagger] + \frac{1}{d}(1-p)\text{Tr}_X[M\mathbb{1}M^\dagger] \quad (10)$$

is a constant channel for all U_λ . This holds iff the first term is independent of λ , and we therefore see that $\{\mathcal{E}_{U_\lambda}^{(p)}\}_\lambda$ can be masked for any $p > 0$ iff the corresponding gates $\{U_\lambda\}_\lambda$ can be masked, for which we turn to Theorem 1 to decide. To investigate more interesting classes of channels, we restrict our attention to qubit systems.

1. Pauli channels

One of the most important types of qubit channels are the Pauli channels, which have the form

$$\mathcal{E}_{\vec{p}}(\cdot) = \sum_i p_i \sigma_i(\cdot) \sigma_i^\dagger \quad (11)$$

for $i = \{0, x, y, z\}$ and probability four-vector $\vec{p} = (p_0, p_x, p_y, p_z)$. Masking of channels $\{\mathcal{E}_{\vec{p}}\}_{\vec{p} \in \mathfrak{M}}$ for arbitrary input state ρ requires that $\text{Tr}_X(M\mathcal{E}_{\vec{p}}(\rho)M^\dagger)$ is fixed for all $\vec{p} \in \mathfrak{M}$, with $X, Y \in \{A, B\}$.

Theorem 2. *Let $\mathfrak{M}$ denote an arbitrary set of probability four-vectors. A family of Pauli channels $\{\mathcal{E}_{\vec{p}}\}_{\vec{p} \in \mathfrak{M}}$ can be masked iff there exists some $k \in \{x, y, z\}$ and constant $c \in [0, 1]$ such that $p_0 + p_k = c$ for all $\vec{p} \in \mathfrak{M}$.*

Proof. ($\Leftarrow$) Suppose without loss of generality that $k = x$ so that $p_0 + p_x = c$. Define the masker $M : \mathbb{C}^2 \rightarrow \mathbb{C}^2 \otimes \mathbb{C}^2$ by $M = |00\rangle\langle +| + |11\rangle\langle -|$, where $|\pm\rangle$ are the ± 1 eigenstates of σ_x . Then a straightforward calculation shows that for any input state ρ we have

$$\begin{aligned} \text{Tr}_X[M\mathcal{E}_{\vec{p}}(\rho)M^\dagger] &= (p_0 + p_x)(|+\rangle\langle +| |0\rangle\langle 0| + |-\rangle\langle -| |1\rangle\langle 1|) \\ &\quad + (p_y + p_z)(|-\rangle\langle -| |0\rangle\langle 0| + |+\rangle\langle +| |1\rangle\langle 1|), \end{aligned}$$

which is the same for all $\vec{p} \in \mathfrak{M}$.

($\Rightarrow$) Suppose that a masker M exists for the channels $\{\mathcal{E}_{\vec{p}}\}_{\vec{p} \in \mathfrak{M}}$. Let us denote action of M on the computational basis as $M|0\rangle = |\Psi_0\rangle_{AB}$ and $M|1\rangle = |\Psi_1\rangle_{AB}$. Then

$$\begin{aligned} \text{Tr}_X[M\mathcal{E}_{\vec{p}}(|0\rangle\langle 0|)M^\dagger] &= (p_0 + p_z)\text{Tr}_X|\Psi_0\rangle\langle \Psi_0| + (p_x + p_y)\text{Tr}_X|\Psi_1\rangle\langle \Psi_1|. \end{aligned}$$

If there exists two vectors $\vec{p}, \vec{p}' \in \mathfrak{M}$ such that $p_0 + p_z \neq p'_0 + p'_z$, then $\text{Tr}_X[M\mathcal{E}_{\vec{p}}(|0\rangle\langle 0|)M^\dagger] = \text{Tr}_X[M\mathcal{E}_{\vec{p}'}(|0\rangle\langle 0|)M^\dagger]$ requires that $\text{Tr}_X|\Psi_0\rangle\langle \Psi_0| = \text{Tr}_X|\Psi_1\rangle\langle \Psi_1|$. Under this assumption, one then computes

$$\begin{aligned} \text{Tr}_X[M\mathcal{E}_{\vec{p}}(|+\rangle\langle +|)M^\dagger] &= \text{Tr}_X|\Psi_0\rangle\langle \Psi_0| + (p_0 + p_x - \tfrac{1}{2})(\text{Tr}_X|\Psi_0\rangle\langle \Psi_1| + \text{h.c.}), \\ \text{Tr}_X[M\mathcal{E}_{\vec{p}}(|\tilde{+}\rangle\langle \tilde{+}|)M^\dagger] &= \text{Tr}_X|\Psi_0\rangle\langle \Psi_0| - i(p_0 + p_y - \tfrac{1}{2})(\text{Tr}_X|\Psi_0\rangle\langle \Psi_1| - \text{h.c.}), \end{aligned} \quad (12)$$

where $|\tilde{+}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$. If there exists two vectors $\vec{p}, \vec{p}' \in \mathfrak{M}$ such that $p_0 + p_x \neq p'_0 + p'_x$, then combining the masking assumption $\text{Tr}_X[M\mathcal{E}_{\vec{p}}(|0\rangle\langle 0|)M^\dagger] = \text{Tr}_X[M\mathcal{E}_{\vec{p}'}(|0\rangle\langle 0|)M^\dagger]$ with the first equality above gives $\text{Tr}_X|\Psi_0\rangle\langle \Psi_1| = -\text{Tr}_X|\Psi_1\rangle\langle \Psi_0|$. Under this further assumption, if there exists two vectors $\vec{p}, \vec{p}' \in \mathfrak{M}$ such that $p_0 + p_y \neq p'_0 + p'_y$, then the second equality above would imply that $\text{Tr}_X|\Psi_0\rangle\langle \Psi_1| = \text{Tr}_X|\Psi_1\rangle\langle \Psi_0|$, which would mean that $\text{Tr}_X|\Psi_0\rangle\langle \Psi_1| = 0$. Yet, it is not possible that

both $\text{Tr}_X|\Psi_0\rangle\langle \Psi_0| = \text{Tr}_X|\Psi_1\rangle\langle \Psi_1|$ and $\text{Tr}_X|\Psi_0\rangle\langle \Psi_1| = 0$. Hence, we have reached a contradiction, and one of our three passing assumptions cannot be true. That is, there must exist some $k \in \{x, y, z\}$ such that $p_0 + p_k$ is constant for all $\vec{p} \in \mathfrak{M}$. $\square$

Example 2. The equality $p_0 + p_k = c$ in Theorem 2 along with normalization imposes two linear constraints on the probability vectors $\vec{p}$. Almost any collection of maskable Pauli channels belongs to a two-parameter family of maskable channels (the exception being the case when $p_0 + p_k = 1$). For example, when $k = X$ and $c < 1$, we have a two-parameter family of maskable channels given by

$$\begin{aligned} \mathcal{E}_{\mu, \nu}(\cdot) &= \mu(\cdot) + (c - \mu)\sigma_X(\cdot)\sigma_X \\ &\quad + \nu\sigma_Y(\cdot)\sigma_Y + (1 - c - \nu)\sigma_Z(\cdot)\sigma_Z \end{aligned} \quad (13)$$

for $\mu \leq c$ and $\nu \leq 1 - c$. This example shows a notable difference between channel and state masking. Namely, every collection of maskable qubit states belongs to a one-parameter family of states corresponding to a circle on the Bloch sphere. In contrast, channel masking allows for multi-parameter families of maskable objects.

2. Any family containing the identity

We now turn to the special problem of masking a channel with the identity, id . As described in the introduction, this has the appealing interpretation of pushing all the noise of a given channel into the correlations between two subsystems, while leaving the reduced state dynamics unaffected. Here, we completely characterize all the qubit channels that allow for such a process. We seek solutions to the equation

$$\text{Tr}_X[M\rho M^\dagger] = \text{Tr}_X[M\mathcal{E}(\rho)M^\dagger], \quad X \in \{A, B\}, \quad \forall \rho. \quad (14)$$

A full solution to this problem for the case of qubit channels is given in the following.

Theorem 3. *The set of qubit channels $\{\text{id}, \mathcal{E}\}$ can be masked iff $\mathcal{E}$ is unital and has a pure state fixed point; i.e. $\mathcal{E}(|\psi\rangle\langle \psi|) = |\psi\rangle\langle \psi|$ for some $|\psi\rangle$.*

Remark 3. Geometrically, we can understand these channels as being maps on the Bloch sphere that preserve the origin as well as two anti-podal points on the surface of the Bloch sphere. The fact that $\mathcal{E}$ is unital with $|\psi\rangle$ as a fixed point means that $|\psi^\perp\rangle$ is also a fixed point, where $|\psi^\perp\rangle$ is orthogonal to $|\psi\rangle$ and satisfying $\mathbb{1} = |\psi\rangle\langle \psi| + |\psi^\perp\rangle\langle \psi^\perp|$.

Remark 4. While Theorem 3 involves masking just a single qubit channel $\mathcal{E}$, it can easily be extended to include more channels. Suppose that $\{\text{id}, \mathcal{E}_\lambda\}_\lambda$ is a family qubit channels that can be masked. Then so can

the pair of channels $\{\text{id}, \sum_{\lambda} p_{\lambda} \mathcal{E}_{\lambda}\}$, where p_{λ} is a probability distribution with $p_{\lambda} > 0$ and chosen such that $\sum_{\lambda} p_{\lambda} \mathcal{E}_{\lambda}(\mathbb{1}) \neq \mathbb{1}$ if one of the channels $\mathcal{E}_{\lambda}$ is non-unital (and arbitrarily chosen otherwise) [22]. By Theorem 3, the convex combination $\sum_{\lambda} p_{\lambda} \mathcal{E}_{\lambda}$ must have a pure-state fixed point. This is possible only if each of the individual channels $\mathcal{E}_{\lambda}$ have the same pure-state fixed point. Moreover, $\sum_{\lambda} p_{\lambda} \mathcal{E}_{\lambda}$ must be unital, which is not possible by our choice of p_{λ} unless all the $\mathcal{E}_{\lambda}$ are unital themselves. We therefore conclude that the $\mathcal{E}_{\lambda}$ must all be unital and have a common pure-state fixed point. Conversely, if all the $\mathcal{E}_{\lambda}$ are unital and have the same pure-state fixed point, then the masker constructed in Lemma 1 below will be a masker for the set $\{\text{id}, \mathcal{E}_{\lambda}\}_{\lambda}$, for the same reason as given in that proof. We summarize in the following.

Corollary 1. *A family of qubit channels $\{\text{id}, \mathcal{E}_{\lambda}\}_{\lambda}$ can be masked iff all the $\mathcal{E}_{\lambda}$ are unital and possess a common pure-state fixed point.*

To prove Theorem 3, we continue with the geometrical picture and recall in more detail that every qubit channel $\mathcal{E}$ can be represented by an affine transformation on the Bloch vectors $\mathbf{n} \rightarrow A\mathbf{n} + \mathbf{b} \in \mathbb{R}^3$ [23]. When the channel is unital (meaning that $\mathcal{E}(\mathbb{1}) = \mathbb{1}$), the vector $\mathbf{b}$ vanishes. The unital case is considered first.

Lemma 1. *If $\mathcal{E}$ is a unital qubit channel, then the set $\{\mathbb{1}, \mathcal{E}\}$ is maskable iff $\mathcal{E}$ has a pure state fixed point; i.e. $\mathcal{E}(|\psi\rangle\langle\psi|) = |\psi\rangle\langle\psi|$ for some $|\psi\rangle$.*

Proof. We begin by noting that a unital channel $\mathcal{E}$ with Bloch sphere action $\mathbf{n} \mapsto A\mathbf{n}$ has a pure-state fixed point iff A has an eigenvalue of $\lambda = 1$. ($\Rightarrow$) Now suppose that $\{\mathbb{1}, \mathcal{E}\}$ is maskable. Let the Bloch sphere action of $\mathcal{E}$ be given by $\mathbf{n} \rightarrow A\mathbf{n}$. We claim that A must have an eigenvalue of $\lambda = 1$. Suppose on the contrary that it does not. Then $A - \mathbb{1}$ is non-singular, and so for any vector $\mathbf{v}$, we can identify the nonzero vector $\mathbf{w} = (A - \mathbb{1})^{-1}\mathbf{v}$ such that $A\mathbf{w} = \mathbf{w} + \mathbf{v}/\|\mathbf{w}\|$, where $\hat{\mathbf{w}} = \mathbf{w}/\|\mathbf{w}\|$. Then

$$\text{Tr}_X[M\mathcal{E}(|\hat{\mathbf{w}}\rangle\langle\hat{\mathbf{w}}|)M^{\dagger}] = \text{Tr}_X[M\frac{1}{2}(\mathbb{1} + \frac{\mathbf{w} + \mathbf{v}}{\|\mathbf{w}\|} \cdot \vec{\sigma})M^{\dagger}],$$

$$\text{Tr}_X[M|\hat{\mathbf{w}}\rangle\langle\hat{\mathbf{w}}|M^{\dagger}] = \text{Tr}_X[M\frac{1}{2}(\mathbb{1} + \frac{\mathbf{w}}{\|\mathbf{w}\|} \cdot \vec{\sigma})M^{\dagger}].$$

The masking conditions of Eq. (14) then implies that $\text{Tr}_X[M(\mathbf{v} \cdot \vec{\sigma})M^{\dagger}] = 0$, which further means that

$$\begin{aligned} \text{Tr}_X[M|\hat{\mathbf{v}}\rangle\langle\hat{\mathbf{v}}|M^{\dagger}] &= \text{Tr}_X[M\frac{1}{2}(\mathbb{1} + \hat{\mathbf{v}} \cdot \vec{\sigma})M^{\dagger}] \\ &= \frac{1}{2}\text{Tr}_X[MM^{\dagger}]. \end{aligned} \quad (16)$$

Since $\hat{\mathbf{v}}$ is arbitrary, and the RHS is independent of $\mathbf{v}$, we see that M would need to be a masker for all qubit states, which is impossible. We therefore conclude that A must have an eigenvalue of $\lambda = 1$, and so $\mathcal{E}$ has a pure-state fixed point.

($\Leftarrow$) Suppose that $\mathcal{E}(|\psi\rangle\langle\psi|) = |\psi\rangle\langle\psi|$. Let U be a unitary such that $U|0\rangle = |\psi\rangle$ such that the conjugated

channel $\mathcal{E}' := \mathcal{U}^{\dagger} \circ \mathcal{E} \circ \mathcal{U}$ has $|0\rangle$ as a fixed point. Since $\{\text{id}, \mathcal{E}\}$ is maskable iff $\{\text{id}, \mathcal{E}'\}$ is maskable, it suffices to prove that the latter set is maskable.

With $|0\rangle\langle 0| = \frac{1}{2}(\mathbb{1} + \sigma_z)$ being a fixed point of $\mathcal{E}'$, the Bloch sphere transformation matrix of $\mathcal{E}'$ will satisfy $A\hat{z} = \hat{z}$ (and so $\mathcal{E}'(\sigma_z) = \sigma_z$). Furthermore, since $\|A\| \leq 1$, the matrix A must have block form

$$A = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

We therefore see that the channel $\mathcal{E}'$ acts invariantly on the $x - y$ plane of the Bloch sphere. With this observation, we can see prove that the simple isometry $M|0\rangle = |00\rangle$ and $M|1\rangle|11\rangle$ serves as a masker for $\{\text{id}, \mathcal{E}'\}$. To see this, note that

$$\begin{aligned} \text{Tr}_X[MM^{\dagger}] &= \mathbb{1}, \quad \text{Tr}_X[M\sigma_z M^{\dagger}] = \sigma_z, \\ \text{Tr}_X[M\sigma_x M^{\dagger}] &= \text{Tr}_X[M\sigma_y M^{\dagger}] = 0. \end{aligned} \quad (17)$$

Then for an arbitrary state $\rho = \frac{1}{2}(\mathbb{1} + \mathbf{n} \cdot \vec{\sigma})$, we have

$$\begin{aligned} \text{Tr}_X[M\mathcal{E}'(\rho)M^{\dagger}] &= \frac{1}{2}\text{Tr}_X[M\mathcal{E}'(\mathbb{1} + \mathbf{n} \cdot \vec{\sigma})M^{\dagger}] \\ &= \frac{1}{2}\text{Tr}_X[MM^{\dagger} + n_z M\sigma_z M^{\dagger} \\ &\quad + M\mathcal{E}(n_x \sigma_x + n_y \sigma_y)M^{\dagger}] \\ &= \frac{1}{2}(\mathbb{1} + n_z \sigma_z), \end{aligned} \quad (18)$$

where the second equality follows from the facts that $\mathcal{E}'$ is unital and $\mathcal{E}'(\sigma_z) = \sigma_z$, while the second equality follows from the facts that $\mathcal{E}'$ acts invariantly on the $x - y$ plane and Eq. (17). At the same time,

$$\begin{aligned} \text{Tr}_X[M\rho M^{\dagger}] &= \frac{1}{2}\text{Tr}_X[MM^{\dagger} + n_z M\sigma_z M^{\dagger} \\ &\quad + M(n_x \sigma_x + n_y \sigma_y)M^{\dagger}] \\ &= \frac{1}{2}(\mathbb{1} + n_z \sigma_z), \end{aligned} \quad (19)$$

where we again use Eq. (17). With ρ be arbitrary, a comparison of Eqns. (18) and (19) shows that M is a masker for $\{\text{id}, \mathcal{E}'\}$. $\square$

To complete the proof of Theorem 3, we now consider the non-unital case.

Lemma 2. *If $\mathcal{E}$ is a non-unital qubit channel, then it is not possible to mask the set $\{\mathbb{1}, \mathcal{E}\}$.*

Proof. Let $\mathcal{E}$ be an arbitrary non-unital channel, and suppose on the contrary that a masker exists for $\{\mathbb{1}, \mathcal{E}\}$. The action of $\mathcal{E}$ on the Bloch sphere is now described by an affine transformation $\mathbf{n} \mapsto A\mathbf{n} + \mathbf{b}$, with $\mathbf{b} \neq 0$. Equivalently, we have $\mathcal{E}(\mathbb{1}) = (1 + \|\mathbf{b}\|)|\hat{\mathbf{b}}\rangle\langle\hat{\mathbf{b}}| + (1 - \|\mathbf{b}\|)|-\hat{\mathbf{b}}\rangle\langle-\hat{\mathbf{b}}|$, where $\hat{\mathbf{b}} = \mathbf{b}/\|\mathbf{b}\|$. At the same time,

$\mathbb{1} = |\hat{\mathbf{b}}\rangle\langle\hat{\mathbf{b}}| + |-\hat{\mathbf{b}}\rangle\langle-\hat{\mathbf{b}}|$. Substituting this into Eq. (14) for the choice $\rho = \mathbb{1}$ gives

$$\begin{aligned} & \text{Tr}_X[M|\hat{\mathbf{b}}\rangle\langle\hat{\mathbf{b}}|M^\dagger] + \text{Tr}_X[M|\hat{\mathbf{b}}\rangle\langle-\hat{\mathbf{b}}|M^\dagger] \\ &= (1 + \|\mathbf{b}\|)\text{Tr}_X[M|\hat{\mathbf{b}}\rangle\langle\hat{\mathbf{b}}|M^\dagger] \\ &+ (1 - \|\mathbf{b}\|)\text{Tr}_X[M|-\hat{\mathbf{b}}\rangle\langle-\hat{\mathbf{b}}|M^\dagger], \end{aligned} \quad (20)$$

which implies

$$\text{Tr}_X[M|\hat{\mathbf{b}}\rangle\langle\hat{\mathbf{b}}|M^\dagger] = \text{Tr}_X[M|-\hat{\mathbf{b}}\rangle\langle-\hat{\mathbf{b}}|M^\dagger] \quad (21)$$

since $\mathbf{b} \neq 0$. This equation says that a masker exists for both states $|\pm\hat{\mathbf{b}}\rangle$. We will now argue that the same masker must also mask even more states, to the point that a contradiction is reached. We distinguish between two cases: (i) the matrix A in the transformation $\mathbf{n} \mapsto A\mathbf{n} + \mathbf{b}$ is not proportional to the identity, and (ii) the matrix A is proportional to the identity.

Case (i): If A is not proportional to the identity, then there exists a unit vector $\hat{\mathbf{c}} \neq \hat{\mathbf{b}}$ such that $A\hat{\mathbf{c}} + \mathbf{b} = t\hat{\mathbf{b}}$ for some scalar t . Indeed, if A is invertible take $\hat{\mathbf{c}} = A^{-1}\mathbf{b}/\|A^{-1}\mathbf{b}\|$ and $t = \|\mathbf{b}\|(1 + 1/\|A^{-1}\mathbf{b}\|)$; if A is non-invertible take $\hat{\mathbf{c}}$ in its kernel and $t = \|\mathbf{b}\|$. Hence, for the inputs $|\hat{\mathbf{c}}\rangle$ we have $\mathcal{E}(|\hat{\mathbf{c}}\rangle\langle\hat{\mathbf{c}}|) = (1+t)/2|\hat{\mathbf{b}}\rangle\langle\hat{\mathbf{b}}| + (1-t)/2|-\hat{\mathbf{b}}\rangle\langle-\hat{\mathbf{b}}|$. From the masking condition and Eq. (21) we find

$$\text{Tr}_X[M|\hat{\mathbf{c}}\rangle\langle\hat{\mathbf{c}}|M^\dagger] = \text{Tr}_X[M|\hat{\mathbf{b}}\rangle\langle\hat{\mathbf{b}}|M^\dagger], \quad (22)$$

We therefore conclude that $\{|\pm\hat{\mathbf{b}}\rangle, |\hat{\mathbf{c}}\rangle\}$ is a set of three distinct maskable states.

Next, there are two unit vectors $\pm\hat{\mathbf{d}}$ that are normal to the plane containing the vectors $\{\pm\hat{\mathbf{b}}, \hat{\mathbf{c}}\}$. Since $\mathcal{E}$ is non-unital, both $|\hat{\mathbf{d}}\rangle\langle\hat{\mathbf{d}}|$ and $|-\hat{\mathbf{d}}\rangle\langle-\hat{\mathbf{d}}|$ cannot be fixed points of $\mathcal{E}$. Assume without loss of generality that $\mathcal{E}(|\hat{\mathbf{d}}\rangle\langle\hat{\mathbf{d}}|) \neq |\hat{\mathbf{d}}\rangle\langle\hat{\mathbf{d}}|$. Since $\{\mathbf{b}, \mathbf{c}, \mathbf{d}\}$ forms a basis for $\mathbb{R}^3$, we can write $A\hat{\mathbf{d}} + \mathbf{b} = w\hat{\mathbf{b}} + y\hat{\mathbf{c}} + z\hat{\mathbf{d}}$ with $\|w\hat{\mathbf{b}} + y\hat{\mathbf{c}} + z\hat{\mathbf{d}}\| \leq 1$ and $|z| < 1$. Hence,

$$\begin{aligned} \mathcal{E}(|\hat{\mathbf{d}}\rangle\langle\hat{\mathbf{d}}|) &= \frac{1}{2}(\mathbb{1} + (w\hat{\mathbf{b}} + y\hat{\mathbf{c}} + z\hat{\mathbf{d}}) \cdot \vec{\sigma}) \\ &= \frac{1}{2}(1 + w - y - z)|\hat{\mathbf{b}}\rangle\langle\hat{\mathbf{b}}| \\ &+ \frac{1}{2}(1 - w - y - z)|-\hat{\mathbf{b}}\rangle\langle-\hat{\mathbf{b}}| + y|\hat{\mathbf{c}}\rangle\langle\hat{\mathbf{c}}| \\ &+ z|\hat{\mathbf{d}}\rangle\langle\hat{\mathbf{d}}|. \end{aligned} \quad (23)$$

The masking condition on $|\hat{\mathbf{d}}\rangle\langle\hat{\mathbf{d}}|$ and $\mathcal{E}(|\hat{\mathbf{d}}\rangle\langle\hat{\mathbf{d}}|)$ implies that

$$(1 - z)\text{Tr}_X[M|\hat{\mathbf{d}}\rangle\langle\hat{\mathbf{d}}|M^\dagger] = (1 - z)\text{Tr}_X[M|\hat{\mathbf{b}}\rangle\langle\hat{\mathbf{b}}|M^\dagger]. \quad (24)$$

Because $|z| < 1$, this equation says that M is capable of masking $|\hat{\mathbf{d}}\rangle$ along with the states $\{|\pm\hat{\mathbf{b}}\rangle, |\hat{\mathbf{c}}\rangle\}$. However, this is a contradiction since the states $\{|\pm\hat{\mathbf{b}}\rangle, |\hat{\mathbf{c}}\rangle, |\hat{\mathbf{d}}\rangle\}$ do not have Bloch vectors that fall on a single disk.

Case (ii): If A is proportional to the identity, then the action of $\mathcal{E}$ is given by $\mathbf{n} \mapsto \lambda\mathbf{n} + \mathbf{b}$ with $|\lambda| < 1$. Hence, $\mathcal{E}(|\hat{\mathbf{n}}\rangle\langle\hat{\mathbf{n}}|) = \lambda|\hat{\mathbf{n}}\rangle\langle\hat{\mathbf{n}}| + \frac{1}{2}((1 - \lambda)\mathbb{1} + \mathbf{b} \cdot \vec{\sigma})$, and so the masking condition says that

$$\begin{aligned} \text{Tr}_X[M|\hat{\mathbf{n}}\rangle\langle\hat{\mathbf{n}}|M^\dagger] &= \lambda\text{Tr}_X[M|\hat{\mathbf{n}}\rangle\langle\hat{\mathbf{n}}|M^\dagger] \\ &+ \frac{1}{2}\text{Tr}_X[M((1 - \lambda)\mathbb{1} + \mathbf{b} \cdot \vec{\sigma})M^\dagger] \\ (1 - \lambda)\text{Tr}_X[M|\hat{\mathbf{n}}\rangle\langle\hat{\mathbf{n}}|M^\dagger] &= \frac{1}{2}\text{Tr}_X[M((1 - \lambda)\mathbb{1} + \mathbf{b} \cdot \vec{\sigma})M^\dagger] \end{aligned} \quad (25)$$

But since the LHS holds for arbitrary $\hat{\mathbf{n}}$ and the RHS is constant, we see that M is a masker for the entire Bloch sphere, which is impossible. $\square$

C. Masking classical channels

We close our study by considering the classical analog of channel masking. A classical channel on discrete sets $\mathcal{X} \rightarrow \mathcal{Y}$ is given by a collection of conditional probability distributions $p(y|x)$, with $x \in \mathcal{X}$ and $y \in \mathcal{Y}$. The corresponding CPTP then has the form $\mathcal{C}(\cdot) = \sum_{x,y} p(y|x)|y\rangle\langle y| \langle x| \cdot |x\rangle$. Moreover, the classical analog of a unitary channel is just a permutation Π .

We first observe that it is impossible for any classical circuit to mask two distinct permutations Π_1 and Π_2 on some set $\mathcal{X} = \{1, 2, \dots, d\}$. Let $|x\rangle$ be such that $\Pi_1|x\rangle = |y\rangle$ and $\Pi_2|x\rangle = |y'\rangle$ with $y \neq y'$. Any reversible classical masker for $\{\Pi_1, \Pi_2\}$ would be a one-to-one mapping $M : \{1, \dots, d\} \mapsto \{1, \dots, d\}^{\times 2}$. However, this means that $M|y\rangle = |z_1\rangle|z_2\rangle$ and $M|y'\rangle = |z'_1\rangle|z'_2\rangle$ for $\{z_1, z_2\} \neq \{z'_1, z'_2\}$. Therefore, the final state for at least one of the subsystems will differ depending on whether Π_1 or Π_2 is applied to input $|x\rangle$; i.e. masking is not possible.

On the other hand, using a quantum masker *any* family of classical channels can be masked.

Lemma 3. *Any family of classical channels with finite input and output sets $\mathcal{X}$ and $\mathcal{Y}$ can be masked by a quantum masker.*

Proof. Let $S = \{\mathcal{C}_\lambda\}_\lambda$ be a collection of classical channels having the form

$$\mathcal{C}_\lambda(\cdot) = \sum_{x \in \mathcal{X}, y \in \mathcal{Y}} p_\lambda(y|x) |x\rangle\langle x| |y\rangle\langle y|. \quad (26)$$

Without loss of generality, suppose $\mathcal{Y} = \{1, 2, \dots, d\}$. We then define a quantum masker $M : \mathbb{C}^d \rightarrow \mathbb{C}^d \otimes \mathbb{C}^d$ for S by its action:

$$M|j\rangle = \frac{1}{\sqrt{d}} \sum_{k=1}^d w^{kj} |kk\rangle \quad (27)$$

where $w = e^{2\pi i/d}$. One can easily verify that the reduced density matrices on subsystems A and B are always maximally mixed, $\mathbb{1}_d/d$. $\square$

III. CONCLUSION

In this paper, we have introduced and developed the concept of quantum channel masking, a dynamical extension of state masking in which the identity of a channel is hidden from local subsystems but remains globally recoverable. We provided a complete characterization of maskable sets of qudit unitary gates $\{U_n\}_{n=1}^N$, showing that masking is possible if and only if $\{U_1^\dagger U_n\}_{n=2}^N$ forms a pairwise commuting set. For the special case of qubit unitaries, we translated this into a geometric picture on the Bloch sphere corresponding to rotational symmetries.

We extended our analysis of channel masking to noisy qubit channels, characterizing all families of maskable Pauli channels. Interestingly, there exists two-parameter families of Pauli channels that can be masked. We further showed that non-unital channels cannot be masked with the identity, whereas certain families of unital qubit channels allow for such masking. This can be interpreted as a scenario in which the effect of noise is completely hidden from each subsystem. Beyond quantum systems, we

showed that while classical channels cannot be masked by classical circuits, quantum maskers can successfully mask any set of arbitrary classical channels. Thus we have demonstrated a clear operational advantage of quantum operations.

Our work establishes a foundation for understanding concealment of quantum operations themselves, with implications in secure quantum information processing including applications in quantum secret sharing [8, 9, 15], error correction [13, 14], and bit commitment [10]. Several promising directions for future research emerge from our findings. A natural extension is to investigate channel masking mixed ancilla states, as we consider only the pure ancilla case. This may broaden the class of maskable channels. Additionally, Modi. et. al. propose a no-qubit commitment protocol based on state masking, in which the committing party can always cheat [10]. It would be of interest to explore the channel masking analogue to this qubit commitment protocol. Finally, extending geometrical interpretations of channel masking beyond qubits to higher-dimensional systems may reveal interesting structural limitations.

-
- [1] W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, *Nature (London)* **299**, 802 (1982).
 - [2] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, Noncommuting mixed states cannot be broadcast, *Phys. Rev. Lett.* **76**, 2818 (1996).
 - [3] A. Kalev and I. Hen, No-broadcasting theorem and its classical counterpart, *Phys. Rev. Lett.* **100**, 210502 (2008).
 - [4] A. Pati and S. Braunstein, Impossibility of deleting an unknown quantum state, *Nature* **404**, 164 (2000).
 - [5] S. L. Braunstein and A. K. Pati, Quantum information cannot be completely hidden in correlations: Implications for the black-hole information paradox, *Phys. Rev. Lett.* **98**, 080502 (2007).
 - [6] D. Kretschmann, D. W. Kribs, and R. W. Spekkens, Complementarity of private and correctable subsystems in quantum cryptography and error correction, *Phys. Rev. A* **78**, 032330 (2008).
 - [7] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, *Rev. Mod. Phys.* **74**, 145 (2002).
 - [8] A. Karlsson, M. Koashi, and N. Imoto, Quantum entanglement for secret sharing and secret splitting, *Phys. Rev. A* **59**, 162 (1999).
 - [9] M. Hillery, V. Bužek, and A. Berthiaume, Quantum secret sharing, *Phys. Rev. A* **59**, 1829 (1999).
 - [10] K. Modi, A. K. Pati, A. Sen(De), and U. Sen, Masking quantum information is impossible, *Phys. Rev. Lett.* **120**, 230501 (2018).
 - [11] X.-B. Liang, B. Li, and S.-M. Fei, Complete characterization of qubit masking, *Phys. Rev. A* **100**, 030304 (2019).
 - [12] F. Ding and X. Hu, Masking quantum information on hyperdisks, *Phys. Rev. A* **102**, 042404 (2020).
 - [13] M.-S. Li and Y.-L. Wang, Masking quantum information in multipartite scenario, *Phys. Rev. A* **98**, 062306 (2018).
 - [14] K. Y. Han, Z. H. Guo, H. X. Cao, Y. X. Du, and C. Yang, Quantum multipartite maskers vs. quantum error-correcting codes, *EPL (Europhysics Letters)* **131**, 30005 (2020).
 - [15] M. Zukowski, A. Zeilinger, M. Horne, and H. Weinfurter, Quest for ghz states, *Acta Physica Polonica A* **93**, 187 (1998).
 - [16] D. Mayers, Unconditionally secure quantum bit commitment is impossible, *Phys. Rev. Lett.* **78**, 3414 (1997).
 - [17] C. E. Shannon, Channels with side information at the transmitter, *IBM Journal of Research and Development* **2**, 289 (1958).
 - [18] H. Boche, N. Cai, and J. Nötzel, The classical-quantum channel with random state parameters known to the sender, *Journal of Physics A: Mathematical and Theoretical* **49**, 195302 (2016).
 - [19] U. Pereg, C. Deppe, and H. Boche, Quantum channel state masking, *IEEE Transactions on Information Theory* **67**, 2245 (2021).
 - [20] H.-K. Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, *Science* **283**, 2050 (1999).
 - [21] I. George, R. Allerstorfer, P. Verduyn Lunel, and E. Chitambar, Orthogonality broadcasting and quantum position verification, *New Journal of Physics* **27**, 054511 (2025).
 - [22] To show that such a p_λ can always be chosen this way, suppose $\mathcal{E}_1(\mathbb{I}) = \sigma \neq \mathbb{I}$ and $p_1 \mathcal{E}_1(\mathbb{I}) + \sum_{i>1} p_i \mathcal{E}_i(\mathbb{I}) = \mathbb{I}$. Then by considering a sufficiently small perturbation $p_1 \mapsto (1-\epsilon)p_1$ and $p_i \mapsto (1+\epsilon \frac{p_1}{1-p_1})p_i$ for $i>1$, we have $(1-\epsilon)p_1 \mathcal{E}_1(\mathbb{I}) + (1+\epsilon \frac{p_1}{1-p_1}) \sum_{i>1} p_i \mathcal{E}_i(\mathbb{I}) = \mathbb{I} - \epsilon \frac{p_1}{1-p_1} (\sigma - \mathbb{I})$, which does not equal the identity for all $\epsilon > 0$.
 - [23] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, 2010).
 - [24] Y. Wang, Z. Hu, B. C. Sanders, and S. Kais, Qudits and high-dimensional quantum computing, *Frontiers in Physics* **8**, 10.3389/fphy.2020.589504 (2020).