Private and Robust States for Distributed Quantum Sensing

Luís Bugalho[1,2,3,4], Majid Hassani[4], Yasser Omar[1,2,3], and Damian Markham[4]

[1]Instituto Superior Técnico, Universidade de Lisboa, Portugal
[2]Physics of Information and Quantum Technologies Group, Centro de Física e Engenharia de Materiais Avançados (CeFEMA), Portugal
[3]PQI – Portuguese Quantum Institute, Portugal
[4]Sorbonne Université, CNRS, LIP6, 4 Place Jussieu, Paris F-75005, France

Jan 8, 2025

arXiv:2407.21701v2 [quant-ph] 9 Jan 2025

Distributed quantum sensing enables the estimation of multiple parameters encoded in spatially separated probes. While traditional quantum sensing is often focused on estimating a single parameter with maximum precision, distributed quantum sensing seeks to estimate some function of multiple parameters that are only locally accessible for each party involved. In such settings, it is natural to not want to give away more information than is necessary. To address this, we use the concept of privacy with respect to a function, ensuring that only information about the target function is available to all the parties, and no other information. We define a measure of privacy (essentially how close we are to this condition being satisfied) and show it satisfies a set of naturally desirable properties of such a measure. Using this privacy measure, we identify and construct entangled resource states that ensure privacy for a given function under different resource distributions and encoding dynamics, characterized by Hamiltonian evolution. For separable and parallel Hamiltonians, we prove that the GHZ state is the only private state for certain linear functions, with the minimum amount of required resources, up to SLOCC. Recognizing the vulnerability of this state to particle loss, we create families of private states, that remain robust even against loss of qubits, by incorporating additional resources. We then extend our findings to different resource distribution scenarios and Hamiltonians, resulting in a comprehensive set of private and robust states for distributed quantum estimation. These results advance the understanding of privacy and robustness in multi-parameter quantum sensing.

Contents

1 Introduction **2**

2 Estimation Scenarios and Privacy **4**
2.1 Resources 7
2.2 Functions of Parameters 8
2.3 Privacy Measure 10

3 Building Private States **12**

3.1 Initial Concepts . . . 13
3.2 Privacy for Stabilizer States with Separable Hamiltonians . . . 15
3.3 Privacy for Arbitrary States with Separable Hamiltonians . . . 18
3.4 Privacy for Arbitrary States with General Hamiltonians . . . 23

4 Robustness **26**
4.1 QFI for Mixed States . . . 26
4.2 Dephasing Noise . . . 27
4.3 Bit-flip Noise . . . 27
4.4 Depolarizing Noise . . . 28
4.5 Amplitude-Damping Noise . . . 29
4.6 Particle Loss . . . 29
4.7 Generalizing Results . . . 31

5 Discussion of the Results **31**

A Unitary Equivalence of Encoding Dynamics **38**

B Privacy Measure **39**

C Integer Vectors Properties **41**

D QFI Matrix for Arbitrary States **42**

E Matrix Rank Inequalities **43**

F Private States - Proofs **44**

G Private States Existence for General Hamiltonians **48**

H QFI for Mixed States - Derivations **50**

1 Introduction

Quantum metrology and quantum sensing have been longstanding areas of interest in quantum information research [1, 2]. In particular, they are known to surpass the classical bounds for the estimation physical parameters in experiments and reach the Heisenberg scaling [1, 3–7]. The idea is that a probe state interacts with some physical process, which encodes parameters into the quantum state of the probe, measuring thereafter and using the outcomes to perform an estimation the parameters. In the case of single parameter estimation, one is interested in estimating one parameter of a system with the maximum precision [3, 8]. However, in the multi-parameter scenario, not only is precision important, but also what information is available. The latter has been directly linked to entangled probes across the sites. With the ongoing development of quantum networks, both over large distances [9–11] and local-area types of networks [12], distributed quantum sensing has emerged as a promising area of research, taking the multiparameter scenario to applications with near-term potential [10, 13–18]. Moreover, there have been some experiments demonstrating the quantum advantage for this setting [5, 19].

Distributed quantum sensing has numerous use cases, such as clock synchronization protocols [20, 21], optical interferometry proposals [22], some preliminary work on gravity and dark-matter experiments [23–26] and physical implementation of sensors capable of

measuring such quantities [27, 28]. One can also find different approaches to solve the optimal estimation of sensing parameters, such as variational quantum sensing [29–31], covert sensing [32, 33], error-corrected [34] and error-mitigated [35] quantum sensing, and controlled enhanced quantum sensing [36].

The framework for distributed quantum sensing has been well-established as quantum sensor networks [10, 13–16, 18, 37–39], where each quantum node holds a set of resources (in our case, qubits) and has access to a local parameter θ_μ (encoded by some local Hamiltonian; see Fig. 1). We are interested in when they want to estimate not the local parameters themselves, but some function of these parameters $f(\{\theta_\mu\}) \equiv f(\boldsymbol{\theta})$. More recently, security concerns have been addressed in several works [33, 40, 41], along with the critical concept of privacy [42]. On the one hand, in a network setting there may be eavesdroppers who want to gain unauthorised access to the value of the parameters, or even simply disrupt or corrupt the estimation process [33, 40, 41]. On the other hand, some parties who are involved in the estimation itself, may like to gain more information than they should - for example the value of other parties local parameters themselves. This is addressed by the notion of privacy, which ensures that, only information about a target estimator can be obtained [42]. Who has access to what information about the parameters typically depends on the initial state used in the estimation scenario, prompting the natural question of identifying private states. In [42] privacy is defined for a specific function (the average value of the parameters), and the questions of general functions, the optimality of the states, and how to deal with noise were left open.

In this work we develop a broad framework for privacy in networks of quantum sensors. We tackle these questions by finding a way to define and quantify privacy through the analysis of the quantum Fisher information (QFI) matrix, a key metric in a quantum estimation scenario [2, 43, 44]. From here we verify that the amount of resources and the control over the dynamics that encode the parameters determine the functions of parameters available at hand. We are able to find a general expression for the QFI matrix of any arbitrary quantum pure state, starting with stabilizer states, in the multi-parameter scenario. We use these results to prove which ones are the only private states, *i.e.* states where the information available is only the target function. Our findings relate the amount of resources and the properties of the encoding dynamics to the functions available at hand for an estimation scenario. In particular, for local and separable encoding dynamics, it will be required a minimum amount of distributed resources to even be able to estimate a target function privately. We generalize our findings for local but not necessarily separable dynamics, by analyzing the eigenvalues of the local Hamiltonians. In creating these families of private states, we then question their robustness against several types of common Pauli noise, and for qubit-loss, which is know to hinder quantum sensing. We find that some of our private states retain information even after particle loss, while at the same time, remaining private.

This paper is structured as follows: we start in Section 2 by analysing the methods commonly used to tackle the problem of multiparameter sensing and define exactly our setup problem as a network problem. This encompasses defining three things beforehand: *(i)* what are the target functions of parameters; *(ii)* defining what are the resources and introducing a notation to deal with them, and finally *(iii)* creating a measure for privacy from a set of premises. In Section 3 we address the problem of finding private states. We start by introducing important concepts and notations to deal with the upcoming problem. Then we present statements about the privacy of states both for stabilizer states and arbitrary pure states for local and separable Hamiltonians, generalizing then to arbitrary local Hamiltonians. We provide conditions for a given function to be private and find the

unique minimum set of private states, give some examples and then provide relaxations of optimality to allow robustness. Finally, in Section 4, we analyze the effect of different noise types over our found families of private states. Over the manuscript we try to be consistent notation wise, using greek letters for nodes, latin letters for individual qubits, boldsymbols to denote a higher dimensional object, wether it be a partition on a set, a vector of parameters or a larger operator decomposed by smaller operators.

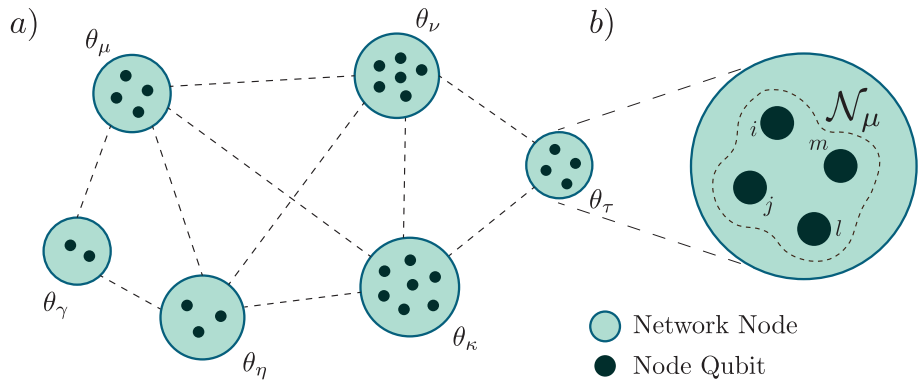


Figure 1: Distributed sensing scenario, consisting of *a)* a network of quantum nodes, capable of distributing entangled states, where *b)* each of the nodes holds their own sets of qubits $\mathcal{N}_\mu$, which can be seen as resources for quantum sensing.

2 Estimation Scenarios and Privacy

There are three important inputs of an estimation scenario: *(i)* the initial state, *(ii)* the encoding dynamics and *(iii)* the measurement (see Fig. 2). Consider first the single parameter case. The initial state is transformed via the encoding dynamics to state ρ_θ, which is then measured giving results x, with probability $p(x|\theta)$, from which one would like to estimate the parameter theta. In the frequentist approach to the estimation problem, we are interested in retrieving information of the parameter over successive measurements. In this scenario, the overall precision of the parameter is bounded by the Fisher information (FI), $F(\theta)$, and the number of measurements made m [2, 8], in the assymptotic regime:

$$\begin{aligned} \Delta\theta^2 &\geq \frac{1}{mF(\theta)} \\ F(\theta) &= \int p(\mathbf{x}|\theta)\left(\partial_\theta \ln p(\mathbf{x}|\theta)\right)^2 d\mathbf{x}. \end{aligned} \tag{1}$$

When the estimation scenario involves a quantum initial state and quantum dynamics, the Fisher information becomes its quantum counterpart. The probability distribution is now given by the Born rule $p(\mathbf{x}|\theta) = \mathrm{Tr}[\Pi_\mathbf{x}\rho_\theta]$, where the set $\{\Pi_\mathbf{x}\}_\mathbf{x}$ denotes a POVM

satisfying $\sum_{\mathbf{x}} \Pi_{\mathbf{x}} = \mathbb{1}$. The quantum version of the FI can then be written as:

$$\begin{aligned}\mathcal{I}(p(\mathbf{x}|\theta)) &= \int p(\mathbf{x}|\theta) \left(\partial_\theta \ln p(\mathbf{x}|\theta)\right)^2 d\mathbf{x} \\ &= \int \frac{1}{p(\mathbf{x}|\theta)} \left(\partial_\theta p(\mathbf{x}|\theta)\right)^2 d\mathbf{x} \\ &= \int \frac{1}{\mathrm{Tr}[\Pi_{\mathbf{x}}\rho_\theta]} \left(\partial_\theta \mathrm{Tr}[\Pi_{\mathbf{x}}\rho_\theta]\right)^2 d\mathbf{x} \\ &= \int \frac{\mathrm{Tr}[\Pi_{\mathbf{x}}\dot{\rho}_\theta]^2}{\mathrm{Tr}[\Pi_{\mathbf{x}}\rho_\theta]} d\mathbf{x},\end{aligned} \tag{2}$$

where $\dot{\rho}_\theta = \frac{\partial \rho_\theta}{\partial \theta}$. By maximising over all POVMs which do not explicitly depend on θ, the quantum Fisher information (QFI), $\mathcal{Q}(\theta)$ appears by implicitly defining an additional operator named the symmetric logarithmic derivative (SLD), and Eq. 1 becomes:

$$\begin{aligned}\Delta\theta^2 &\geq \frac{1}{m\mathcal{Q}(\theta)} \\ \mathcal{Q}(\theta) &= \mathrm{Tr}\left[\rho_\theta L_{\rho_\theta}^2\right], \quad \partial_\theta \rho_\theta = \frac{\rho_\theta L_\theta + L_\theta \rho_\theta}{2},\end{aligned} \tag{3}$$

which is often denoted by quantum Crámer-Rao bound. Note that achieving this bound might only be achievable by implementing POVMs that depend on the target θ [8], requiring adaptive schemes. However, for some of the private states we will find, this should not pose a problem, as the optimal POVM is known to be θ-independent. The QFI depends on the state of the system immediately before measurement, meaning it will depend on the initial state of the system and the dynamics of the encoding (and additional sources of noise which we leave for discussion on the robustness section of this work). Eq. 3 has a simpler counterpart for the case of pure states, as in this case the SLD is simply given by $L_\theta = 2\partial_\theta \rho_\theta$:

$$\mathcal{Q}(\rho_\theta) = 4\mathrm{Re}\left\{\langle \partial_\theta \psi_\theta | \partial_\theta \psi_\theta \rangle - \langle \partial_\theta \psi_\theta | \psi_\theta \rangle \langle \psi_\theta | \partial_\theta \psi_\theta \rangle\right\}. \tag{4}$$

In quantum sensing, and in particular in the distributed scenario, the goal is often to estimate a function of parameters that are spatially distributed. This means that the dynamics that encode the parameters are in spatially separated locations and the resources only have access to their own local dynamics. The natural way of addressing this problem is in a network, where each channel encoding one parameter is associated with one node. While the structure of the network impacts the initial state distribution, it does not impact the overall estimation scenario. Given a graph $G = (V, E)$, in a distributed scenario we consider a set of nodes $\{\mu \in V(G) = 1, 2, \cdots, k\}$, each of them with access to some quantum dynamics described by a quantum channel $\Lambda_{\theta_\mu}(\rho)$ (if unitary, this is described by a Hamiltonian), which encodes its own parameter θ_μ, as we outline in Fig. 1.

In this case, the QFI becomes more complex as it involves multiple parameters. Given that the Crámer-Rao bound is a bound on the variance, in the multi-parameter scenario, the variance becomes a covariance matrix. Therefore, it makes sense that the QFI is also a matrix. The description follows naturally from Eq. 1 by substituting $\partial_\theta \to \partial_{\theta_\mu}, \partial_{\theta_\nu}$. In this way, the SLD is now defined with respect to one parameter L_{θ_μ} and the Crámer-Rao bound and QFI matrix entries are given by [2, 10, 44, 45]:

$$\begin{aligned}COV(\boldsymbol{\theta}) &\geq \frac{1}{m}\boldsymbol{\mathcal{Q}}(\boldsymbol{\theta})^{-1}, \\ \boldsymbol{\mathcal{Q}}_{\mu\nu}(\rho_{\boldsymbol{\theta}}) &= \mathrm{Tr}\left[\rho_{\boldsymbol{\theta}} \frac{L_{\theta_\mu} L_{\theta_\nu} + L_{\theta_\nu} L_{\theta_\mu}}{2}\right], \quad \partial_{\theta_\mu} \rho_\theta = \frac{\rho_\theta L_{\theta_\mu} + L_{\theta_\mu} \rho_\theta}{2},\end{aligned} \tag{5}$$

where $A \geq B$ is meant in the sense that $A-B$ is a semi-definite positive matrix. Expanding for pure states where $\rho_{\boldsymbol{\theta}} = |\psi_{\boldsymbol{\theta}}\rangle\langle\psi_{\boldsymbol{\theta}}|$, just as in Eq. 4 using $L_{\theta_\mu} = 2\partial_{\theta_\mu}\rho_{\boldsymbol{\theta}}$, one can verify that the QFI simplifies to:

$$\boldsymbol{\mathcal{Q}}_{\mu\nu}(\rho_{\boldsymbol{\theta}}) = 4\mathrm{Re}\left\{\langle\partial_{\theta_\mu}\psi_{\boldsymbol{\theta}}|\partial_{\theta_\nu}\psi_{\boldsymbol{\theta}}\rangle - \langle\partial_{\theta_\mu}\psi_{\boldsymbol{\theta}}|\psi_{\boldsymbol{\theta}}\rangle\langle\psi_{\boldsymbol{\theta}}|\partial_{\theta_\nu}\psi_{\boldsymbol{\theta}}\rangle\right\}. \tag{6}$$

Since each node only has access to its own parameters in distributed scenarios, it is reasonable to assume the encoding dynamics are local and unitary (see Fig. 2). Under these assumptions over the encoding dynamics, there are still multiple scenarios one can analyze (see Fig. 2). Let us detail the most general one given in Fig. 2c :

$$\Lambda_{\theta_\mu}(\rho) = e^{-i\theta_\mu \boldsymbol{H}_\mu}, \quad \boldsymbol{H}_\mu = \sum_{P_j\in\mathcal{P}_\mu} b_j P_j, \quad \mathcal{P}_\mu = \{P\in\mathcal{P}_n : P = \bigotimes_{j\notin\mu}\mathbb{1}_j \bigotimes_{j\in\mu}\sigma_j\}, \tag{7}$$

where $\mathcal{P}_n$ is the set of all Pauli strings with size n, which is the total amount of qubits (see subsection detailing the notation for resources further ahead). Note that the Pauli strings of size n form an orthogonal basis for the vector space of complex $2^n \times 2^n$ matrices. Although this description can be quite general, what is usually the subject of sensing scenarios are channels which are local and separable for each qubit [10, 38](see Fig. 2b):

$$\Lambda_{\theta_\mu}(\rho) = e^{-i\theta_\mu \boldsymbol{G}_\mu}, \quad \boldsymbol{G}_\mu = \sum_{j\in\mu} G_j, G_j \equiv \mathbb{1}\otimes\cdots\otimes G_j\otimes\cdots\otimes\mathbb{1} \implies \Lambda_{\theta_\mu}(\rho) = \bigotimes_{j\in\mu} e^{-i\theta_\mu G_j}, \tag{8}$$

where we did not fixed a given generator of translation for any qubit, *i.e.* the operators G_j are described by $\vec{x}\cdot\vec{\sigma}$, where $\vec{x}\in\mathbb{R}^3$ is normalized, and $\vec{\sigma}$ is the Pauli vector. As it is known, the Pauli group on 1 qubit exponentiates to the unitary group on 1 qubit $U(2)$ [46]. This consists on the most general local and separable encoding dynamics, where each qubit acquires the phase once. One can also refer to this case as parallel, in the sense that if every qubit encoding is separable from one another, then each local encoding can be done at the same time, in parallel, and consequently so can the global dynamics. If one were to consider more general encoding dynamics, such as the case in Eq. 7 and Fig. 2c, one may arrive at a problem that quickly becomes infeasible, and the definition of sampling the system starts to drift. This is due to the fact that, for separable dynamics, one might argue that each qubit goes through the parameter channel only once, or is sampled only one time [47]. With more complex Hamiltonians, this is not always the case. Some Hamiltonians cannot be directly rewrote into only one access to a channel for each qubit. We will discuss this case further, and provide a statement to building private states for a given arbitrary Hamiltonian.

Nonetheless, for separable encoding dynamics, even though we do not fix the generators G_j, we can reduce the problem complexity by fixing the dynamics and resorting to the following lemma:

Lemma 2.1. *Consider two different generators for single qubit unitary operators G and G', and a unitary operator W.*

$$\forall G, G'; \exists W : W^\dagger G W = G'$$

Corollary 2.1 (Interplay Dynamics $\leftrightarrow$ Initial State)**.** *Consider two different unitary encodings, in terms of two different generators $U_\theta = e^{-i\theta G}$ and $U'_\theta = e^{-i\theta G'}$, and a unitary operator W.*

$$\forall U_\theta, U'_\theta; \exists W : W^\dagger U_\theta W = U'_\theta$$

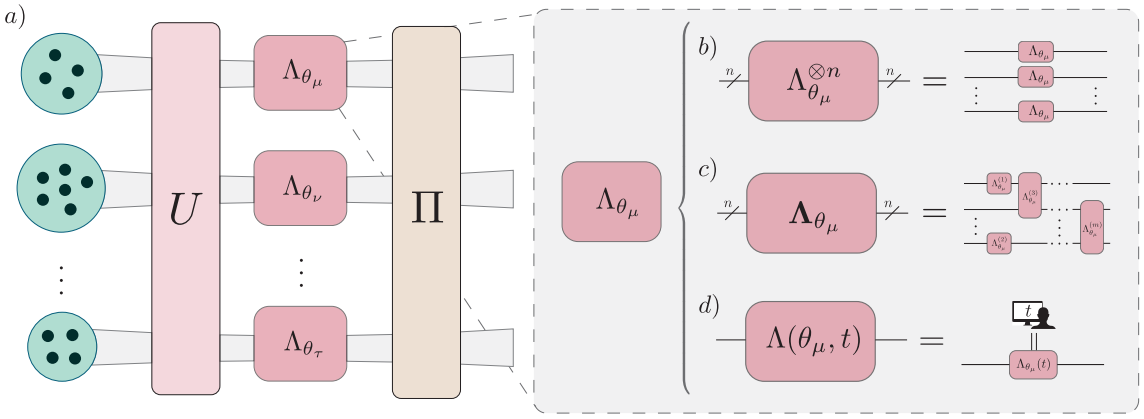


Figure 2: Quantum circuit description of the estimation scenario. *a* Each network node qubits' have access only to their encoding dynamics, which imprint each of the parameters θ_μ locally. Nonetheless, the initial state is not bounded to local states, they can be arbitrarily entangled between all the sets of qubits, illustrated above as a global entanglement preperation unitary U, and so can the final POVM Π. We divide the local encoding dynamics into three types: *b)* parallel single-qubit dynamics (or separable); *c)* most general non-controllable dynamics and *d)* one-qubit controllable dynamics, where a extra parameter t is provided by the user.

Both Lemma 2.1 and Corollary 2.1 can be intuitively thought as changing the local definition of each qubit's basis from the regular basis $\{|0\rangle, |1\rangle\}$ to the eigenbasis of the generators G given by $\{|g\rangle, |-g\rangle\}$, where $G|\pm g\rangle = \pm|\pm g\rangle$. We provide proofs for the above lemma and corollary in Appendix A. From Corol. 2.1 we get that changing the dynamics is equivalent to changing the initial state locally, and vice-versa. This in turn means that, for every separable dynamics we are always able to find a state with access to the same information, by applying a local unitary gate. This allows us to fix either one part or the other when trying to optimize the estimation. Because of this, we will often fix the local dynamics to a unitary of the type $e^{i\theta\sigma_j}$ where σ_j is a Pauli operator (we will choose Z whenever we need to), and say that the initial state attaining a certain estimation outcome is equivalent up to a certain local-unitary (LU) operation.

2.1 Resources

Unlike the single parameter scenario of quantum sensing, in distributed sensing the resources are spatially distributed over a structure resembling a network, hence the name quantum sensor networks [10, 14, 15, 18]. To convey their distribution over the nodes (or parties), it makes sense to have a notation that attributes a corresponding node to each qubit. The ensemble of qubits constitutes the set of resources for the estimation scenario, even though one could, equivalently, consider the amount of samples or duration of access to the encoding dynamics. The case where the encoding dynamics are not separable is more involved. We will comment further on this over Section 3.4, but for now let us define the number of resources in terms of amount of the qubits available locally.

Introducing the notation for the resources sets we will use throughout the paper: we denote by $\mathcal{N}_\mu$ as the set of qubits (or local resources) belonging to node μ (see Fig. 1), which amounts to the total set of qubits given by $\mathcal{N} = \cup_{\mu=1}^{k}\mathcal{N}_\mu$. For this reason, we denote $\boldsymbol{\mathcal{N}} = \{\mathcal{N}_\mu\}_{\mu\in V}$ as a partition of the set, corresponding to the distributed resources. Moreover, the number of qubits in each set is given by $|\mathcal{N}_\mu| = n_\mu$, which means the vector $\vec{n} = (n_1, n_2, \cdots, n_k)$ is the vector of resources and $|\mathcal{N}| = \|\vec{n}\|_1 = n$ is the total amount

of resources. Moreover, we will assume that the states can be picked from the complete Hilbert space of all qubits, which we denote by $\mathcal{H}(\mathcal{N})$.

Another important aspect that will be used throughout the paper, is to be able to order different vectors, such as the vector of resources. Since we are usually working with a vector-space defined over some ordered ring, we resort to the regular product order, which has appeared in quantum information under the name of majorization as well (e.g. [48]), defined as follows:

Definition 2.1. *Let $\mathbb{K}$ be a ordered-ring and $H \subseteq \mathbb{K}^k$. Let $\vec{a}, \vec{b}$ be two vectors belonging to H. Let $\leq$ be a total order of the field $\mathbb{K}$. The product order is defined as:*

$$\vec{a} \preceq \vec{b} \qquad \textit{iff.} \qquad a_j \leq b_j \ \forall j \in \{1, 2, \cdots, k\}.$$

Moreover, we say $\vec{a} \prec \vec{b}$ if $\vec{a} \preceq \vec{b}$ and $\exists j : (\vec{a})_j < (\vec{b})_j$.

Note that unlike $\leq$, $\preceq$ is not a total order, *i.e.* there are vectors such that neither $\vec{a} \preceq \vec{b}$ nor $\vec{b} \preceq \vec{a}$. In this case we use the notation $\vec{a} \npreceq \vec{b}$.

Example 2.1.

$$(2,4,3) \preceq (2,4,3) \quad , \quad (2,4,3) \prec (2,6,4) \quad , \quad (1,3,2) \npreceq (3,2,4)$$

2.2 Functions of Parameters

Before discussing the bounds on the precision and information metrics, let us first clear up the idea of what is the "good" definition for functions of parameters. The first thing to notice is the following: if one is able to estimate $f(\boldsymbol{\theta})$, then one can also estimate $\alpha f(\boldsymbol{\theta})$ for any α. For this reason, let us establish an equivalence between functions: we say $f(\boldsymbol{\theta}) \sim g(\boldsymbol{\theta})$ if $f(\boldsymbol{\theta}) = \alpha g(\boldsymbol{\theta})$ for some α. Since we are working with linear functions of parameters, the functions can be described as an inner-product between a vector of coefficients and a vector of the parameters $\boldsymbol{\theta}$: $f(\boldsymbol{\theta}) = \vec{a} \cdot \vec{\boldsymbol{\theta}}$, similarly to previous works [10, 14, 38, 42].

As we will see in this paper, the linear coefficients available are somehow related with the eigenvalues of the Hamiltonian. For this reason, we start by finding a way to describe them, that is able to convey the distributed scenario we are working with. Taking the most general local Hamiltonians description in Eq. 7, one can find an orthonormal basis for the local states by choosing the eigenvectors of the local Hamiltonians. Associated to each of these eigenvectors we then have their corresponding eigenvalues, which we can arrange as follows:

$$\boldsymbol{H}_\mu \left|\lambda_j^\mu\right\rangle = \lambda_j^\mu \left|\lambda_j^\mu\right\rangle, \quad \mathcal{B}^\mu = \{\left|\lambda_j^\mu\right\rangle\}_{i \in \mu}, \quad \mathcal{O}^\mu = \{\lambda_j^\mu\}_{j \in \mu}, \tag{9}$$

where $\mathcal{B}^\mu$ is a local basis for the qubits belonging to node μ, and $\mathcal{O}^\mu$ is the list of non-identical eigenvalues for the local Hamiltonian of node μ. Note that this list does not have the same size as the basis if the Hamiltonian is degenerate, although this will not pose any problem.

Going from the local Hamiltonians to the full network states can be easily done by choosing an orthonormal basis from the tensor product of the local basis:

$$\left|\lambda_{\vec{j}}\right\rangle = \bigotimes_\mu \left|\lambda_{j_\mu}^\mu\right\rangle, \quad \boldsymbol{H}_\mu \left|\lambda_{\vec{j}}\right\rangle = \lambda_{j_\mu}^\mu \left|\lambda_{\vec{j}}\right\rangle, \quad \mathcal{B} = \bigotimes_\mu \mathcal{B}^\mu, \quad \mathcal{O} = \prod_\mu \mathcal{O}^\mu, \tag{10}$$

where the vector $\vec{j}$ is a labeling vector such that each component $(\vec{j})_\mu \equiv j_\mu$ corresponds to one of the local basis states of node μ. Moreover, the set $\mathcal{O}$ can be seen as a discrete subset of the k-orthotope $\overline{\mathcal{O}}$ defined by $[\lambda_{\min}^1, \lambda_{\max}^1] \times \cdots \times [\lambda_{\min}^k, \lambda_{\max}^k]$.

As we will verify further ahead, the natural functions one can estimate correspond to vectors living inside of the k-orthotope $\overline{\mathcal{O}}$. We will start by analyzing the case of separable dynamics and later generalize the most general encoding dynamics. For separable dynamics we have that:

1. *Controlled scenario*: $\vec{a} \in \mathbb{R}^k$ – we are able to control the local encoding dynamics by an additional parameter t, $\Lambda = \Lambda(\theta, t) = \Lambda(\theta t) \sim e^{i\theta t \sigma_j}$ (see Fig. 2 d);

2. *Non-controlled scenario*: $\vec{a} \in \mathbb{Z}^k$ – only the local number of qubits per node or party is controllable ($\Lambda = \Lambda(\theta) \sim e^{i\theta\sigma_j}$).

Note that from the equivalence of functions introduced above, any $f(\boldsymbol{\theta}) = \vec{a} \cdot \vec{\boldsymbol{\theta}}$ such that $\vec{a} \in \mathbb{Q}^k$ is equivalent to some $g(\boldsymbol{\theta}) = \vec{a}' \cdot \vec{\boldsymbol{\theta}}$ such that $\vec{a}' \in \mathbb{Z}^k$. This extends the *non-controlled scenario* to not only integers, but also fractionals. However, there will exist an overhead in the amount of resources. This overhead can be calculated from finding the smallest number α one has to multiply $\vec{a}$ such that $\alpha\vec{a} = \vec{a}' \in \mathbb{Z}^k$, which is given by the least common multiplier of all denominators. This depends entirely on the vector $\vec{a}$.

For the *controlled scenario* one can establish an equivalence with the *non-controlled*, by taking one qubit in every node ($\vec{n} = \vec{1}$) and control each local parameter t_μ in order to get $\vec{a}$. One can additionally change $\vec{n}$ and $\vec{t}$ such that $n_\mu t_\mu = a_\mu$, and get to the same result. This should provide that any statement made for the *non-controlled scenario* should also verify for the *controlled scenario*. On the other hand, in the *non-controlled scenario*, we are limited by the number of qubits in each node, which only takes values over the integers. Taking the quotient of the equivalence relation, we get that, in this case, it suffices to analyse functions such that every element of $\vec{a}$ has no greatest common divisor than 1. For this we introduce the following definition:

Definition 2.2. *Let $\vec{a}$ be a integer vector of size k, $\vec{a} \in \mathbb{Z}^k, \vec{a} = (a_1, a_2, \cdots, a_k)$.*

$$gcd(\vec{a}) = gcd(a_1, a_2, \cdots, a_k) = gcd(a_1, gcd(a_2, \ldots, gcd(a_{k-1}, a_k)))$$

Where gcd is the greatest common divisor of a set of integer numbers.

This means that the representative of each equivalence class of functions has $\vec{a}$ such that $gcd(\vec{a}) = 1$. Note the results for arbitrary $\vec{a}$ verifying $gcd(\vec{a}) = 1$ work backwards for $\vec{n} = \vec{1}$ in the *controlled scenario*.

In the *non-controlled scenario*, let $\vec{a}$ and $\vec{n} \in \mathbb{Z}^k$ be the vector of the target function and the vector of resources, respectively. From here on, when we refer to the vector of the target function $\vec{a}$, we will assume that $gcd(\vec{a}) = 1$. Using this ordering, let us define four different regions of amount of resources:

(I) $\vec{n} \prec \vec{a}$ or $\vec{n} \not\preceq \vec{a}$ (No-Privacy Zone)

(II) $\vec{n} = \vec{a}$ (Minimal Privacy Zone)

(III) $\vec{a} \prec \vec{n}$ and ($\vec{n} \prec 2\vec{a}$ or $\vec{n} \not\preceq 2\vec{a}$) (Minimal plus Ancilla Privacy Zone)

(IV) $2\vec{a} \preceq \vec{n}$ (Multiple Privacy Zone)

The labeling will become obvious as we will be able to prove different statements for each zone.

2.3 Privacy Measure

The privacy of a quantum estimation scenario, given a target linear function was introduced in [42]. In a distributed estimation scenario, a private state allows each party to access the information given only by the target function. This means that while the parties can jointly estimate the target function, they cannot infer each other's individual parameters.

More generally, we consider a set of malicious parties, which we label D for dishonest, and the remaining set of parties is labeled H for honest. The honest parties will follow the protocol as instructed, and the dishonest parties can work together, and along with the source, in any way they like (bounded only by quantum mechanics) to try to find out as much information as possible. Privacy for networked parameter estimation means that the dishonest set can only access the information of the agreed target function, and their local parameters (and any combinations thereof). More concretely, this leads to the definition of privacy as:

(i) If all parties are honest, they can estimate $f(\boldsymbol{\theta})$.

(ii) For any set of dishonest parties D, the set D can only know the function $f(\boldsymbol{\theta})$ and all θ_μ for $\mu \in D$ (and functions thereof).

This definition is inspired from similar definitions for privacy in secure multiparty computation [42]. Note that, as in multiparty computation, dishonest sets can always conspire to give a distorted value of the target function $f(\boldsymbol{\theta})$. Though this possibly feels like a failure, there is little one could hope to do against that, as they are valid members of the network. For example, one could simply follow the protocol but add an extra phase on their system to distort the value of $f(\boldsymbol{\theta})$. There would be no way of detecting this as different from the phase that was actually desired (see e.g. [49]). What is important is that the dishonest parties do not get information about the honest parties parameters any more than is agreed on by the target global function.

To motivate the construction of the a privacy measure, let us first describe one property of the QFI matrix. Given that a linear function can be described as $f(\vec{\boldsymbol{\theta}}) = \vec{a} \cdot \vec{\boldsymbol{\theta}}$, one can always construct a non-unique orthonormal basis that includes the vector $\vec{a}/\|\vec{a}\|$ and defines a unitary transformation. Call this matrix A, where every vector belongs to one orthonormal basis. Then:

$$\vec{\boldsymbol{\theta}}' = A\,\vec{\boldsymbol{\theta}} \qquad \text{with } \theta'_1 = \sum_i A_{1i}\theta_i = \frac{\vec{a}}{\|\vec{a}\|} \cdot \vec{\boldsymbol{\theta}} \sim f(\vec{\boldsymbol{\theta}}). \tag{11}$$

Since the QFI depends on the derivatives, which change through linear transformations, finding the new derivatives is straightforward:

$$\frac{\partial}{\partial \theta'_i} \to \sum_j \frac{\partial \theta_j}{\partial \theta'_i}\frac{\partial}{\partial \theta_j} \implies \nabla_{\vec{\boldsymbol{\theta}}'} \to A^T \cdot \nabla_{\vec{\boldsymbol{\theta}}'}. \tag{12}$$

This in turn implies that the QFI changes in the following way when changing variables [8, 44]:

$$\begin{aligned}
\mathcal{Q}'_{ij}(\rho_{\boldsymbol{\theta}}) &= \int \frac{1}{\mathrm{Tr}[\Pi_{\mathbf{x}}\rho_\theta]} \partial_{\theta'_i}\left(\mathrm{Tr}[\Pi_{\mathbf{x}}\rho_\theta]\right) \partial_{\theta'_j}\left(\mathrm{Tr}[\Pi_{\mathbf{x}}\rho_\theta]\right) d\mathbf{x} \\
&\downarrow \\
\mathcal{Q}'_{ij}(\rho_{\boldsymbol{\theta}}) &= \sum_{k,l} \int \frac{1}{\mathrm{Tr}[\Pi_{\mathbf{x}}\rho_\theta]} A^T_{ik}\partial_{\theta_k}\left(\mathrm{Tr}[\Pi_{\mathbf{x}}\rho_\theta]\right) A^T_{jl}\partial_{\theta_l}\left(\mathrm{Tr}[\Pi_{\mathbf{x}}\rho_\theta]\right) d\mathbf{x} \\
&\downarrow \\
\mathcal{Q}'(\rho_{\boldsymbol{\theta}}) &= A^T \mathcal{Q} A.
\end{aligned} \tag{13}$$

This has an interesting consequence: by calculating the QFI for the canonical $\boldsymbol{\theta}$ set of parameters, and then diagonalizing the matrix we are finding the linear transformation that retrieves the set of independent orthonormal parameters that the estimation scheme is sensitive to. This means the eigenvectors of the QFI matrix correspond to the natural set of functions available at hand given the estimation scenario, and their corresponding eigenvalues are the precision at which we can estimate them. Note however, that this does not mean that every function precision is always attainable, given the not-guaranteed commutation of the measurements which would allow one to saturate the Cramér-Rao bound [50]. Nonetheless, this allows to introduce a notion of privacy - having a rank-1 QFI matrix, with the only positive eigenvector spanning the space of the target function. Note that a rank-1 matrix is naturally non-invertible, making the multiparameter Crámer-Rao bound in Eq. 5 ill-defined, as all the functions belonging to the null-space of the matrix would have an associated infinite variance. This aligns with the fact that these functions cannot be estimated, as they are not accessible. One could make use of a pseudo-inverse to address this fact, or transform the problem into a single-parameter scenario by applying a weight matrix in the vector direction [45]. It is also important and useful to be able to quantify such a property - no state will perfectly satisfy such a condition due to inevitable noise, for example. It is then important to be able to say how close we are to being private. Although in [42] privacy is quantified for the special case considered there, it is not general, not easily calculable, and its precise meaning in terms of the information leaked is not clear.

With this in mind, we list some properties that are naturally desirable for a measure if one is to quantify how close one is to being perfectly private:

1. $\mathcal{P} = \mathcal{P}(\mathcal{Q}, \vec{a})$ where: *(i)* $\mathcal{Q}$ is the QFI matrix with respect to parameters $\boldsymbol{\theta} = \{\theta_1, \theta_2, ..., \theta_k\}$, and provides the available information of the estimator and *(ii)* $\vec{a}$ is the vector that defines the target function $f(\boldsymbol{\theta}) = \vec{a} \cdot \vec{\boldsymbol{\theta}}$.

2. $\mathcal{P}(\mathcal{Q}, \vec{a}) \in [0, 1]$ to allow for normalization. The measure should depend not on the amount of information, nor the target vector norm, but on how the information is aligned with the target function.

3. $\mathcal{P}(\mathcal{Q}, \vec{a}) = 1$ iff. $\mathcal{Q} = \alpha \vec{a}\vec{a}^T$, meaning if and only if the information is aligned with the target function, then a state is completely private, with respect to that same function.

4. $\mathcal{P}(B\mathcal{Q}B^T, B\vec{a}) = \mathcal{P}(\mathcal{Q}, \vec{a})$ as changing the basis should be equivalent to changing the target function. This is motivated by linear transformations of the parameters not changing the information available, in the rotated corresponding linear function.

5. $\forall \epsilon > 0, A \geq 0, \ \exists \delta > 0 : |\mathcal{P}(\mathcal{Q} + \epsilon A, \vec{a}) - \mathcal{P}(\mathcal{Q}, \vec{a})| \leq \delta$ to ensure that continuity of the QFI implies the continuity of the privacy.

Property 1 and 3 ensure that the information available of a quantum estimation procedure (provided by $\mathcal{Q}$) align solely with the target function. Property 2 is a matter of defining the values this measure can take. Property 4 asserts that any linear reassignment of the parameters does not change the privacy statement for the new parameters. Finally, property 5 allows for a statement of the continuity of quantum states implying continuity of the privacy measure, as we know that if a quantum state is close to another, so is the QFI matrix [60]. This is a set of necessary properties for a measure able to characterize and distinguish different quantum estimation procedures, with respect to the linear subspace of the obtained information. We now present our privacy measure, which satisfies these properties:

Definition 2.3. *The privacy measure of a multi-parameter estimation problem, which results in a quantum Fisher information matrix $\mathcal{Q}$, with respect to a target linear function $f(\vec{\boldsymbol{\theta}}) = \vec{a} \cdot \vec{\boldsymbol{\theta}}$ with $||\vec{a}|| = 1$ is given by:*

$$\mathcal{P}(\mathcal{Q}, \vec{a}) = \frac{\vec{a}^T \mathcal{Q} \vec{a}}{\operatorname{Tr} \mathcal{Q}} \equiv \frac{\operatorname{Tr}\left[\mathcal{Q}\vec{a}\vec{a}^T\right]}{\operatorname{Tr} \mathcal{Q}} = \frac{\operatorname{Tr}\left[\mathcal{Q} W_{\vec{a}}\right]}{\operatorname{Tr} \mathcal{Q}}.$$

In case $||\vec{a}|| \neq 1$, simply redefine $\vec{a} = \vec{a}/||\vec{a}||$.

In Appendix B we prove that the privacy measure in Def. 2.3 verifies all the proposed properties, and address as well the meaning behind the numerical value of $\mathcal{P}$. Nonetheless, we provide some intuition below:

1. $\mathcal{P} = 1$, means complete privacy, and in particular a state that verifies this is guaranteed to satisfy all conditions.

2. For $\mathcal{P} = 0$, this implies there is a function of parameters, orthogonal to the target function $f(\boldsymbol{\theta})$, that the dishonest parties can access optimally, which by the privacy condition (iii), the dishonest parties should have no information of. On the other hand, if everybody is honest, no information about $f(\boldsymbol{\theta}) = \vec{a} \cdot \vec{\boldsymbol{\theta}}$ could possibly be obtained.

3. If $\mathcal{P} = \epsilon$, then one can do the same as above, but less efficiently, *i.e.* the best strategy can only gather less information about the same function than when $\mathcal{P} = 0$. In particular, the amount of information accessible decreases with the increase of ϵ, which is equivalent to needing more repetitions to get the same variance on the information available.

We note here that in our setting the dynamics are part of the problem setting, so that privacy above depends only on the state, hence the notion of private state. The idea of the private sensing protocols of [42] is to certify that one possesses such a private state, then use it for sensing, in this way ensuring privacy. Our definition of privacy contains several implications for a distributed secure sensing protocol. As a consequence of the definition of privacy, if one certifies a private state, then one is able to guarantee that a private estimation protocol is also completely secure [42]. All the private states we find here can be certified using the techniques of [42, 51], and so can be included into protocols, guaranteeing private sensing.

3 Building Private States

To build private states, we start by developing an efficient way to characterize the QFI matrix as a function of the input state and fixed separable and parallel dynamics, first for stabilizer states using the stabilizer formalism, and next taking an arbitrary state as input, by choosing an appropriate basis. Using Corol. 2.1 this generalizes to any local single-qubit (or separable) dynamics, up to some local single-qubit operation. Later we will extend into the case of the most general dynamics, by finding another basis with respect to the more general encoding dynamics. Using this, and applying the privacy definition, we are able to prove which states and superpositions of states will be private ($\mathcal{P} = 1$), allowing us to create families of private states. Moreover, we do this in function of the amount of resources, as one will see is key to being able to find private states.

3.1 Initial Concepts

Before diving into building private states, let us introduce some well-known concepts and adaptations of them, that allow us to build the tools for our proofs of privacy. Starting with the Hamming-weight, a function that, given a bit string, outputs the number of ones of the string:

Definition 3.1. *Let s be a string of bits of size n, $s \in \mathbb{F}_2^n$. The Hamming weight of s, $h(s)$ is given by:*

$$h(s) = \sum_{j=1}^{n} s_j.$$

Note, one key property of the Hamming-weight is its invariance under permutations of bits within the string s:

Proposition 3.1. *Let $X = \{1, 2, ..., n\}$ be the set of positions of a bit string s of size n. Let S_X be the permutation group over X.*

$$h(s) = h(\sigma(s)) \quad \forall \sigma \in S_X, \forall s$$

This in fact allows one to create equivalence classes on binary strings for the Hamming-weight, as permutations generate the group that results in the invariance of the Hamming weight:

$$\begin{array}{ccccc} s \in & & \mathbb{F}_2^n & & \\ & & \sigma \downarrow & \searrow^{h} & \\ [s] \in & & \mathbb{F}_2^n/S_X & \xrightarrow[\tilde{h}]{} & \mathbb{Z} \end{array}$$

Where $\tilde{h}$ is an isomorphism. This means that doing the quotient $\mathbb{F}_2^n$ over S_X will create the equivalent classes under the Hamming-weight. We denote them $[s]$, and they constitute the objects in $\mathbb{F}_2^n/S_X$ which are unequivocally mapped to a weight under the Hamming-weight map. For us it is also useful to define a slight variant of the Hamming weight, which we call the symmetrized Hamming-weight:

Definition 3.2. *Let s be a string of bits of size n, $s \in \mathbb{F}_2^n$. The symmetrized Hamming weight of s, $h^*(s)$ is given by:*

$$h^*(s) = \sum_{j=1}^{n} (-1)^{s_j}.$$

Moreover, these two weight-functions are related via a linear transformation:

$$h^*(s) = n - 2 \cdot h(s), \tag{14}$$

where n is the integer size of the set of indices (or the length of the bit string). Because we are in a multiparameter scenario, where the parties have access to different amounts of resources, let us define a new vectorial Hamming-weight. We call it vectorial since in this case, it outputs a vector of Hamming-weights. Using the notation introduced before for the partition of the set of resources:

Definition 3.3. *Let s be a string of bits of size n, $s \in \mathbb{F}_2^n$. Let $\boldsymbol{\mathcal{N}} = \mathcal{N}_1 \cup \cdots \mathcal{N}_k$ be a size k partition over the set of indices of the bit string s, such that $n_j = |\mathcal{N}_j|$, and $\sum_j n_j = n$. Define the $\boldsymbol{\mathcal{N}}$-Hamming weight of s, $\vec{h}_{\boldsymbol{\mathcal{N}}}(s)$ by:*

$$\left(\vec{h}_{\boldsymbol{\mathcal{N}}}(s)\right)_j = \sum_{i \in \mathcal{N}_j} s_i,$$

where j runs from 1 to k, meaning $\vec{h}_{\boldsymbol{\mathcal{N}}}(s) \in \mathbb{Z}^k$.

In the same way one can define its symmetrized counterpart and rewrite the linear relation between them:

$$\vec{h}^*_{\boldsymbol{\mathcal{N}}}(s) = \vec{n} - 2 \cdot \vec{h}_{\boldsymbol{\mathcal{N}}}(s). \tag{15}$$

What before was invariance under any permutation of the bit string, now becomes only under a restricted set of permutations. Let us define this subset and prove that the vectorial Hamming weight is invariant under this subset of permutations.

Definition 3.4. *Let S_X be the permutations group over a set X. Moreover, let $\boldsymbol{X} = \{X_j\}_{j=1,2,\dots,k}$ be a partition of X. Define $S_{\boldsymbol{X}} \subseteq S_X$ as:*

$$S_{\boldsymbol{X}} = S_{X_1} \times S_{X_2} \times \cdots \times S_{X_k}.$$

Proposition 3.2. *Let X be a set and $\boldsymbol{X} = \{X_j\}_{j=1,2,\dots,k}$ be a partition of X. Let S_X be the permutation group over X and $S_{\boldsymbol{X}}$ the subset of it defined according to Def. 3.4.*

$$\vec{h}_{\boldsymbol{X}}(s) = \vec{h}_{\boldsymbol{X}}(\sigma(s)) \quad \forall \sigma \in S_{\boldsymbol{X}}$$

Prop. 3.1 is simply a consequence of the commutativity of the sum. The proof of Prop. 3.2 is a direct consequence of Prop. 3.1 into each of the subsets of the partition. Similarly to before, one can create the equivalence classes of the vectorial Hamming weight. Let us denote them $[s]_{\boldsymbol{X}}$, which are again the objects in $\mathbb{F}_2^n/S_{\boldsymbol{X}}$ which are unequivocally mapped to a weight under the vectorial Hamming weight map.

$$\begin{array}{ccccc} s \in & & \mathbb{F}_2^n & & \\ & & \sigma \downarrow & \searrow^{\vec{h}_{\boldsymbol{X}}} & \\ [s]_{\boldsymbol{X}} \in & & \mathbb{F}_2^n/S_{\boldsymbol{X}} & \xrightarrow[\tilde{h}_{\boldsymbol{X}}]{} & \mathbb{Z}^k \end{array}$$

As an example of using the vectorial Hamming weight and its equivalence classes, consider the following bit strings:

Example 3.1. *Let $\vec{n} = \{1, 3, 2\}$ be a vector in $\mathbb{N}^3$ and $s_1, s_2, s_3 \in \mathbb{F}^6$ be given by $s_1 = 1\ 110\ 10, s_2 = 1\ 101\ 10, s_3 = 1\ 011\ 01$.*

$$\vec{h}_{\boldsymbol{\mathcal{N}}}(s_1) = \vec{h}_{\boldsymbol{\mathcal{N}}}(\underbrace{1}_{\mathcal{N}_1}\underbrace{110}_{\mathcal{N}_2}\underbrace{10}_{\mathcal{N}_3}) = \{h(1), h(110), h(10)\} = \{1, 2, 1\}$$

$$\vec{h}_{\boldsymbol{\mathcal{N}}}(s_1) = \vec{h}_{\boldsymbol{\mathcal{N}}}(s_2) = \vec{h}_{\boldsymbol{\mathcal{N}}}(s_3) \implies [s_1]_{\boldsymbol{\mathcal{N}}} = [s_2]_{\boldsymbol{\mathcal{N}}} = [s_3]_{\boldsymbol{\mathcal{N}}}$$

This means that all bit strings s_1, s_2, s_3 belong to the same equivalence class. Moreover, as a direct consequence of this, there exists necessarily a permutation in $S_{\boldsymbol{\mathcal{N}}}$ that transforms each one into each other one.

One can then show that any bit string s, indexed by a set $\mathcal{N}$, with partition $\boldsymbol{\mathcal{N}}$ with correspondent resource vector $\vec{n}$ has a $\boldsymbol{\mathcal{N}}$-Hamming weight bounded by:

$$\vec{0} \preceq \vec{h}_{\boldsymbol{\mathcal{N}}}(s) \preceq \vec{n} \qquad \implies \qquad -\vec{n} \preceq \vec{h}^*_{\boldsymbol{\mathcal{N}}}(s) \preceq \vec{n}. \tag{16}$$

We also have the following consequences for vectors of integers, which we prove in Appendix C and that will later be crucial:

Proposition 3.3. *$\forall\ \vec{a}, \vec{b} \in \mathbb{Z}^k$ such that $gcd(\vec{a}) = 1$ then, if $\vec{b} = \alpha\vec{a}$ implies that $\alpha \in \mathbb{Z}$.*

Proposition 3.4. *Let $\vec{m}$ be a integer vector in $\mathbb{Z}_+^k$ such that $gcd(\vec{m}) = 1$. Then:*

$$\nexists\ \vec{a} \neq \vec{b} \in \mathbb{Z}_+^k, \vec{a}, \vec{b} \prec \vec{m} : (\vec{m} - 2\vec{a}) \pm (\vec{m} - 2\vec{b}) = \alpha\vec{m} \quad , \quad \alpha \neq 0.$$

Proposition 3.5. *Let $\vec{m}$ be a target vector in $\mathbb{Z}_+^k$ such that $gcd(\vec{m}) = 1$. Let $\vec{n}$ be a resource vector in the same space, such that $\vec{n} \not\succeq \vec{m}$. Then:*

$$\nexists\ \vec{a} \neq \vec{b} \in \mathbb{Z}_+^k, \vec{a}, \vec{b} \prec \vec{n} : (\vec{n} - 2\vec{a}) \pm (\vec{n} - 2\vec{b}) = \alpha\vec{m} \quad , \quad \alpha \neq 0.$$

All of these concepts we have introduced focus on describing the functions available by employing integer resources in an estimation scenario. The manipulation of the Hamming weight into its symmetrized counterpart is a direct consequence (together with Corol. 2.1) of being able to choose any local basis for each qubit. If one is able to choose any basis for one qubit, then each basis will have two possible qubit eigenstates, which can be characterized by a bit (0 or 1), and will have eigenvalues ± 1. Then, each eigenstate of the entire state in such basis can be labeled by a bit string of the size of the number of qubits. Since we choose the basis in the same "direction" as the individual Hamiltonians, then the eigenvectors of the local Hamiltonian will be given by the eigenstates created. Moreover, and as a consequence of the ± 1 eigenvalues of each qubit Hamiltonian, each eigenstate characterized by the bit string s will have a correspondent eigenvalue given by the symmetrized Hamming weight of that bit string. We will use this to prove then how to find the private states, and build the entire set of private states.

3.2 Privacy for Stabilizer States with Separable Hamiltonians

Stabilizer formalism is a very useful formalism to describe quantum states in terms of their symmetries [52–54]. As the name suggests, it involves the notion of a stabilizer, an operator that stabilizes a state ($S|\psi\rangle = |\psi\rangle$). A n-qubit state is called a stabilizer state if it is stabilized by a set of n stabilizers $s \in \mathcal{S}$ such that:

(i) $[s_i, s_j] = 0, \forall s_i, s_j \in \mathcal{S}$ (Abelian),

(ii) $\forall s_i, s_j, s_k \in \mathcal{S} : s_i \circ s_j \neq s_k$ (Linear Independence),

(iii) $s_i \in \{\pm 1, \pm i\}\mathcal{P}^n$ such that $s_i \neq \mathrm{id}$ (Pauli strings).

We will denote the ensemble of stabilizer states in the Hilbert space $\mathcal{H}$ by $\mathsf{Stab}(\mathcal{H})$. Given these conditions, the group generated by $\mathcal{S}$ is the complete set of stabilizers of the state. We call this group $\boldsymbol{S} = \langle \mathcal{S} \rangle$. It is also known that:

$$|\psi\rangle\langle\psi| = \frac{1}{2^n} \sum_{s \in \boldsymbol{S}} s = \frac{1}{2^n} \prod_{s_i \in \mathcal{S}} (\mathbb{1} + s_i). \tag{17}$$

Moreover, there are multiple representations for the generators of a state. We present an example of GHZ state with three qubits, in different representations, namely a stabilizer table representation and the binary sympletic representation:

$\boldsymbol{q}_1$	$\boldsymbol{q}_2$	$\boldsymbol{q}_3$
X_1	X_2	X_3
Z_1	Z_2	$\mathbb{1}$
Z_1	$\mathbb{1}$	Z_3

or $$(\boldsymbol{X}|\boldsymbol{Z}) = \left(\begin{array}{ccc|ccc} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{array}\right). \tag{18}$$

One can easily check that a star-graph centered on the first node is related with the GHZ state of three qubits via Hadamard gates being applied to both leafs of the star-graph, *i.e.* nodes 2 and 3. Doing so is equivalent to applying Hadamard gates to $\boldsymbol{q}_2$ and $\boldsymbol{q}_3$:

$$|GHZ_3\rangle \xrightarrow{H_2H_3} |S_3\rangle$$

$$\begin{array}{ccc} \boldsymbol{q}_1 & \boldsymbol{q}_2 & \boldsymbol{q}_3 \\ \hline\hline X_1 & X_2 & X_3 \\ Z_1 & Z_2 & \mathbb{1} \\ Z_1 & \mathbb{1} & Z_3 \end{array} \xrightarrow{H_2H_3} = \begin{array}{ccc} \boldsymbol{q}_1 & \boldsymbol{q}_2 & \boldsymbol{q}_3 \\ \hline\hline X_1 & Z_2 & Z_2 \\ Z_1 & X_2 & \mathbb{1} \\ Z_1 & \mathbb{1} & X_3 \end{array} \equiv \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{array}\right),$$

where the binary sympletic representation becomes $(\boldsymbol{X}|\boldsymbol{Z}) = (\mathbb{1}|\boldsymbol{\Gamma})$, with $\boldsymbol{\Gamma}$ being the adjacency matrix of the star graph. In general, one can always do this for a graph state.

Using the stabilizer formalism, one can then find an expression for the QFI in terms of the number of stabilizers [43, 55, 56]. Under the assumptions in Eq. 8:

$$\begin{aligned} |\psi_{\boldsymbol{\theta}}\rangle = U_{\boldsymbol{\theta}}\,|\psi\rangle = \bigotimes_{\mu\in V} e^{-i\theta_\mu \boldsymbol{G}_\mu}\,|\psi\rangle\,, \quad |\partial_{\theta_\mu}\psi_{\boldsymbol{\theta}}\rangle = -i\boldsymbol{G}_\mu U_{\boldsymbol{\theta}}\,|\psi\rangle\,, \\ \mathcal{Q}_{\mu\nu}(\rho_{\boldsymbol{\theta}}) = 4\mathrm{Re}\left\{\langle\partial_{\theta_\mu}\psi_{\boldsymbol{\theta}}|\partial_{\theta_\nu}\psi_{\boldsymbol{\theta}}\rangle - \langle\partial_{\theta_\mu}\psi_{\boldsymbol{\theta}}|\psi_{\boldsymbol{\theta}}\rangle\langle\psi_{\boldsymbol{\theta}}|\partial_{\theta_\nu}\psi_{\boldsymbol{\theta}}\rangle\right\} \\ = 4\mathrm{Re}\left\{\langle\psi|\boldsymbol{G}_\mu\boldsymbol{G}_\nu|\psi\rangle - \langle\psi|\boldsymbol{G}_\mu|\psi\rangle\langle\psi|\boldsymbol{G}_\nu|\psi\rangle\right\} \\ = 4\sum_{j\in\mu}\sum_{k\in\nu}\mathrm{Re}\left\{\langle\psi|G_jG_k|\psi\rangle - \langle\psi|G_j|\psi\rangle\langle\psi|G_k|\psi\rangle\right\} \\ = 4\sum_{j\in\mu}\sum_{k\in\nu}\mathrm{id}_{\mathcal{S}_\psi}(G_jG_k) - \mathrm{id}_{\mathcal{S}_\psi}(G_j)\mathrm{id}_{\mathcal{S}_\psi}(G_k), \end{aligned} \tag{19}$$

where $\mathrm{id}_{\mathcal{S}_\psi}(G)$ is the indicator function over the stabilizer set of $|\psi\rangle$, $\mathcal{S}_\psi$, evaluating to 1 if $G \in \mathcal{S}_\psi$ and 0 otherwise. From here we can use the stabilizer formalism to understand which terms come out different from zero. There are two cases one should analyze:

1. If both aG_j and bG_k, where $a, b \in \{\pm 1, \pm i\}$, are stabilizers of the state ψ, then so is abG_jG_k, making its contribution to the QFI null;

2. The only scenario for which the QFI is different from zero is the case where $\pm G_jG_k$ is a stabilizer (note the real part in Eq. 19), but neither aG_j nor bG_k are stabilizers of the state.

The case where either aG_j or bG_k is a stabilizer and $\pm G_jG_k$ is also a stabilizer is not possible, as it would imply all of them are stabilizers. The QFI then becomes a combinatorial problem. The generators G_j can always be made up such that $G_j^p = G_j^{p \mod 2}$, which is the same type of structure when working with the vector space of $\mathbb{F}_2^n$, where the sum is already made modulus 2. Suppose the following set of generators:

$$g(\vec{l}) = G_1^{l_1} \otimes G_2^{l_2} \otimes \cdots \otimes G_n^{l_n}, \tag{20}$$

where $\vec{l} = (l_1, l_2, ..., l_n)$ is a vector in $\mathbb{F}_2^n$, made up of zeros and ones. Using this, we can define the trivial base of n vectors that generate all vectors of $\mathbb{F}_2^n$ by simply:

$$\mathfrak{B}_e \begin{cases} e_1 &= (1,0,0,...,0,0) \\ e_2 &= (0,1,0,...,0,0) \\ &\vdots \\ e_n &= (0,0,0,...,0,1) \end{cases}. \tag{21}$$

From the vector space characteristics, the choice of basis is not unique. This means that taking $\{g(\vec{e}_j)\}_{\vec{e}_j \in \mathfrak{B}_e}$ for our stabilizer generators is equivalent to taking any other basis $g(\vec{\tilde{e}}_j)$, resulting in all terms G_j and $G_j G_k$ being part of the stabilizers of the state. Note that, from its construction using only G_j and $\mathbb{1}$, the commutation rule for the set of generators is already verified. This means that:

Proposition 3.6. *Any generator set of stabilizers in the form of Eq. 20 with an associated complete basis for the binary vectors defines a state with no information retrievable.*

Proof. For a generator set to correspond to a state with information, it should contain terms of the form $G_j G_k$ but not the terms of the form G_j nor G_k. Since there is an isomorphism between the group of stabilizers $\mathcal{S}$ and the $\mathbb{F}_2^n$, any linear independent set of vectors in $\mathbb{F}_2^n$ defines a linear independent set of generators for $\mathcal{S}$. Moreover, taking whichever complete linearly independent basis for $\mathbb{F}_2^n$ we verify that its span includes all bit strings with length n. This in turn implies that whichever basis we choose for Eq. 20, it will include both terms of the form $G_j G_k$ and G_j or G_k, resulting in a state with no information. □

This allows us to prove which states are able to remain private for estimating a family of functions. The following two theorems essentially tell us that the only private stabiliser state resource is locally equivalent to the GHZ state, and the distributed resources (number of qubits per network node) is fixed by the function. We start by proving there is a zone of resources where no private state can be built:

Theorem 3.1 (No-Privacy Zone for Stabilizer States)**.** *Let $\vec{a}, \vec{n} \in \mathbb{Z}^k$, $n = \|\vec{n}\|_1$, $gcd(\vec{a}) = 1$ and $f(\boldsymbol{\theta})$ be the linear function given by $f(\boldsymbol{\theta}) = \vec{a} \cdot \vec{\boldsymbol{\theta}}$. Then, there is no stabilizer state capable of estimating f privately with $\vec{n}$ distributed resources and access to local separable dynamics $U_{\boldsymbol{\theta}}$, such that $\vec{n} \prec \vec{a}$ or $\vec{n} \not\preceq \vec{a}$.*

$$\nexists\, |\psi\rangle \in \mathsf{Stab}(\mathcal{H}(n)) : \mathcal{P}(\mathcal{Q}(U_{\boldsymbol{\theta}} |\psi\rangle), \vec{a}) = 1$$

Note we have only considered the amount of qubits per node, and not the more general qubits distribution using the partition notation $\boldsymbol{\mathcal{N}}$. We follow with the proof:

Proof. Privacy, $\mathcal{P} = 1$, is equivalent to having a QFI matrix given by $\boldsymbol{\mathcal{Q}} = \lambda_1 \cdot \vec{a}\vec{a}^T$ where we can observe a rank one matrix in the direction of $\vec{a}$. Given that the number of operators G_j for each node μ is an integer number bounded by the amount of qubits in that same node n_μ, the maximum of $\boldsymbol{\mathcal{Q}}_{\mu\nu}$ is given by $n_\mu n_\nu$. From the conditions stated one can say that $\exists \mu : n_\mu < a_\mu$. However, by construction a_μ has no common divisors but 1 with all the other a_ν. Since Prop. 3.3 only allows λ_1 to be integer, one could never achieve $\vec{a}\vec{a}^T$. For this reason, whichever basis ends up maximizing the privacy of parameter $\vec{a} \cdot \vec{\boldsymbol{\theta}}$ has a projection onto $\vec{a}$ plus a non-null projection onto at least another linearly independent vector, making it not completely private. □

This already states we require a minimum amount of resources per node to achieve privacy. Next we prove that the first private state requires at least $\vec{n} = \vec{a}$ amount of resources:

Theorem 3.2 (Minimal Privacy Zone for Stabilizer States)**.** *Let $\vec{a}, \vec{n} \in \mathbb{Z}^k$, $gcd(\vec{a}) = 1$ and $f(\boldsymbol{\theta})$ be the linear function given by $f(\boldsymbol{\theta}) = \vec{a} \cdot \vec{\boldsymbol{\theta}}$. Then, there is only one stabilizer state, up to LU operations, capable of estimating f privately with $\vec{n} = \vec{a}$ distributed resources and access to local separable dynamics $U_{\boldsymbol{\theta}}$.*

Proof. Take Corol. 2.1 to deal with LU and use $G_j, G_j^\perp$ as the non-commuting dual of generators for each qubit. Given that $\vec{n} = \vec{a}$, then the only possibility to be private is if every $G_j G_k \in \boldsymbol{\mathcal{S}}$, as one can only find integer multiples of $\vec{a}$ when $gcd(\vec{a}) = 1$ (Prop. 3.3). Consider the table of stabilizers given by:

$$\mathcal{S} = \begin{pmatrix} \boldsymbol{G} \\ \boldsymbol{G}^\perp \end{pmatrix} = \left(\begin{array}{ccccc} G_1 & \mathbb{1} & \mathbb{1} & \cdots & G_n \\ \mathbb{1} & G_2 & \mathbb{1} & \cdots & G_n \\ \vdots & \vdots & & \ddots & \vdots \\ \mathbb{1} & \mathbb{1} & \mathbb{1} & G_{n-1} & G_n \\ \hline G_1^\perp & G_2^\perp & G_3^\perp & \cdots & G_n^\perp \end{array}\right). \tag{22}$$

Note the choice of $\boldsymbol{G}$ is not unique, but if generated via Eq. 20 we cannot use a complete basis (see Prop. 3.6). By enforcing condition 2, one may arrive at $\boldsymbol{G}$, given that all $G_j G_k \in \langle \boldsymbol{G} \rangle$ and no $G_j \in \langle \boldsymbol{G} \rangle$. If one would add $G_j \notin \boldsymbol{G}$, then $\exists G_j G_k \in \langle \boldsymbol{G} \rangle : G_j G_k \circ G_j = G_k \; \forall \; k$ which means a state with zero information. If one would remove a stabilizer from $\boldsymbol{G}$, then $\exists G_p : G_p G_q \notin \boldsymbol{\mathcal{S}} \; \forall \; q$, meaning a non private state. The only option is then to add a new stabilizer that commutes with every other in $\boldsymbol{G}$ and is linearly independent of them. This can only happen by choosing a different orthogonal generator and every element of the generator must be the same, hence: $\boldsymbol{G}^\perp = a G_1^\perp G_2^\perp \cdots G_n^\perp$, $a \in \{\pm 1, \pm i\}$. Up to unitary equivalence (see Corol. 2.1), this defines one state (up to LU) which is able to remain private. □

Note that this state is LU equivalent to the GHZ state. Additionally, our statements are only valid if our stabilizers and generators $G_j, G_j^\perp$ belong to the Pauli strings, as it is required by the stabilizer definition. With the help of Corol. 2.1 one can always work with $G_j = Z, G_j^\perp = X$ and then up to LU, not necessarily still a stabilizer state, the statements above are true.

3.3 Privacy for Arbitrary States with Separable Hamiltonians

To build an arbitrary state, one needs an orthonormal basis of quantum states. The choice of basis is not fixed, which allows to choose whichever preferred basis. If one chooses the basis that contains a state that is LU equivalent to a GHZ state, the calculations become rather straightforward. For this, one can pick the generator set in Eq. 22 as a representation of our state which is LU equivalent to a GHZ state. Since we are no longer working with just stabilizer states, let $G_j, G_j^\perp$ have arbitrary definitions $G_j = \vec{a} \cdot \vec{\sigma}, G_j^\perp = \vec{b} \cdot \vec{\sigma}$ such that $\|\vec{a}\| = \|\vec{b}\| = 1$ and $\vec{a} \cdot \vec{b} = 0$. In particular, one can and should choose the generators of the encoding dynamics, meaning that the G_js should be local generators in Eq. 8. Call this state, represented by the stabilizer table in Eq. 22, $|\mathcal{G}_1\rangle$.

Then, one can think of a generator set of a state as a n subspace of $\mathbb{F}_2^{2n}$ with the help of the symplectic notation introduced in Eq. 18. This means there still exists another subspace of dimension n, orthogonal to the first. One can use this orthogonal subspace to generate the set of orthogonal states, and the orthogonality conditions will appear naturally. In a more concrete way, take the following generator set:

$$\mathcal{S}^\perp = \begin{pmatrix} G_1^\perp & \mathbb{1} & \cdots & \mathbb{1} & \mathbb{1} \\ \mathbb{1} & G_2^\perp & \cdots & \mathbb{1} & \mathbb{1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbb{1} & \mathbb{1} & \cdots & G_{n-1}^\perp & \mathbb{1} \\ \mathbb{1} & \mathbb{1} & \cdots & \mathbb{1} & G_n \end{pmatrix}. \tag{23}$$

This means one can describe an orthornormal basis as $\{|\mathcal{G}_j\rangle = \tilde{s}_j |\mathcal{G}_1\rangle\}_{\tilde{s}_j \in \langle \mathcal{S}^\perp \rangle}$ with 2^n elements, as $|\langle \mathcal{S}^\perp \rangle| = 2^n$. To prove orthonormality take:

$$\langle \mathcal{G}_i | \mathcal{G}_j \rangle = \langle \mathcal{G}_1 | \tilde{s}_i \tilde{s}_j |\mathcal{G}_1\rangle = \mathrm{Tr}[\tilde{s}_i \tilde{s}_j |\mathcal{G}_1\rangle \langle \mathcal{G}_1|] = \frac{1}{2^N} \sum_{s_k \in \langle \mathcal{S} \rangle} \mathrm{Tr}[\tilde{s}_i \tilde{s}_j s_k] = \delta_{ij}. \tag{24}$$

We now decompose an arbitrary state $|\psi\rangle$ over our resources in this basis

$$|\psi\rangle = \sum_j \alpha_j |\mathcal{G}_j\rangle . \tag{25}$$

Using this, we can find a simple expression for the QFI matrix (see derivation over Appendix D) using the notation introduced for our distributed qubits, namely using the partition $\boldsymbol{\mathcal{N}}$ with correspondent vector of resources given by $\vec{n}$:

$$\boldsymbol{\mathcal{Q}}(\rho_{\boldsymbol{\theta}}) = C \boldsymbol{\mathfrak{Q}} C^T, \quad \boldsymbol{\mathfrak{Q}} = \Lambda - \vec{v}\vec{v}^T, \tag{26}$$

where C is a matrix that can be made such that each line i ranges from $i = 0, \ldots, 2^{n-1} - 1$ is given by the corresponding vectorial Hamming-weight of the index i, $\vec{h}^*_{\boldsymbol{\mathcal{N}}}(i) = \vec{n} - 2\vec{c}_i$, with $\vec{0} \preceq \vec{c}_i \prec \vec{n}$. The matrix $\boldsymbol{\mathfrak{Q}}$ is a rank-1 correction of a diagonal matrix, namely $\Lambda = diag(\lambda_0, ..., \lambda_j, ..., \lambda_n)$ and $\vec{v} = (v_0, ..., v_j, ..., v_n)$, such that $\lambda_j \geq |v_j|$ for all j. The structure of this decomposition is exactly what allows us to prove the privacy statements we will make. We will be able to establish bounds on the rank of the QFI matrix using this fact, together with a few additional theorems and propositions we detail in Appendix E.

As we have seen before, the functions at disposition are limited by the amount of resources used, so to provide the limits, we have defined privacy in terms of resources. Let us make a statement for each possible zone introduced in the Resources section (Sec. 2.1). Note that in the previous section we had limited ourselves to states described by stabilizers. In this section we perform equivalent statements on privacy, but for arbitrary pure states, not necessarily limited to stabilizers. The first result is that we still cannot find a private state in the *No privacy zone*:

Theorem 3.3 (No privacy zone)**.** *Let $\vec{a}, \vec{n} \in \mathbb{Z}^k$, $n = \|\vec{n}\|_1$, $gcd(\vec{a}) = 1$ and $f(\boldsymbol{\theta})$ be the linear function given by $f(\boldsymbol{\theta}) = \vec{a} \cdot \vec{\boldsymbol{\theta}}$. Then, there is no pure state capable of estimating f privately with $\vec{n}$ distributed resources and access to local separable dynamics $U_{\boldsymbol{\theta}}$, such that $\vec{n} \prec \vec{a}$ or $\vec{n} \not\preceq \vec{a}$.*

$$\nexists\, |\psi\rangle \in \mathcal{H}(n) : \mathcal{P}(\mathcal{Q}(U_{\boldsymbol{\theta}} |\psi\rangle), \vec{a}) = 1$$

Proof. The privacy is only zero if $\mathcal{Q}(U_{\boldsymbol{\theta}} |\psi\rangle) = \alpha \vec{a}\vec{a}^T \equiv \mathcal{Q}$. From Eq. 26, take the support of $\mathfrak{Q}$, $\mathrm{supp}\, \mathfrak{Q}$ as the sub-matrix with the lines and columns such that $\lambda_j \neq 0$. Moreover, let $C_{\mathrm{supp}\, \mathfrak{Q}}$ be the correspondent sub-matrix of C in the $\mathrm{supp}\, \mathfrak{Q}$, *i.e.* the lines multiplying by the non-zero values of $\mathfrak{Q}$. Note that $\vec{a} \notin C$, and, in particular, $\vec{a} \notin C_{\mathrm{supp}\, \mathfrak{Q}}$. This is a consequence of $\vec{n} \prec \vec{a}$ or $\vec{n} \not\preceq \vec{a}$. Look at the following table covering all possible combinations of outcomes:

rank $\mathrm{supp}\, \mathfrak{Q}$	rank $C_{\mathrm{supp}\, \mathfrak{Q}}$	rank $C \mathfrak{Q} C^T$	Reasoning	Privacy
any	1	≤ 1	$\vec{a} \notin C_{\mathrm{supp}(\mathfrak{Q})}$	Never
dim $\mathrm{supp}\, \mathfrak{Q}$	≥ 2	≥ 2	Prop. E.1	Never
dim $\mathrm{supp}\, \mathfrak{Q}$-1	2	1 or 2	Prop. E.2	Check
dim $\mathrm{supp}\, \mathfrak{Q}$-1	> 2	> 1	Prop. E.2	Never

The only case to check is that of rank $\operatorname{supp}\mathfrak{Q} = \dim \operatorname{supp}\mathfrak{Q} - 1$ with rank $C_{\operatorname{supp}\mathfrak{Q}} = 2$. According to Thm. E.1, $\mathfrak{Q} = diag(\vec{\lambda}) - \vec{\lambda}\vec{\lambda}^T$, up to a matrix made up of ± 1 in the diagonal, call it D. That means the vector $D\vec{1}$ spans the null space, therefore the positive eigenvectors of $\mathfrak{Q}$ are spanned by the orthogonal subspace of $D\vec{1}$, call it $P^{\perp}$. So, take the set of vectors $W = \{\vec{w} | \vec{w} = 1/\sqrt{2}(\vec{e}_i - \vec{e}_j), i \neq j\}$. Notice that the $\mathsf{span}(DW) = \mathsf{span}(P^T)$ as $\langle D\vec{w}; D\vec{1}\rangle = 0 \; \forall w \in W$. Using Prop. E.3 we can analyse then the vectors in DW, which are simpler to check:

$$D\vec{w}C_{\operatorname{supp}\mathfrak{Q}} = 1/\sqrt{2}\left(\vec{h}^*_{\boldsymbol{\mathcal{N}}}(i) \pm \vec{h}^*_{\boldsymbol{\mathcal{N}}}(j)\right) = \begin{cases} 2/\sqrt{2}\left[\vec{n} - \left(\vec{h}_{\boldsymbol{\mathcal{N}}}(i) + \vec{h}_{\boldsymbol{\mathcal{N}}}(j)\right)\right] \\ 2/\sqrt{2}\left(\vec{h}_{\boldsymbol{\mathcal{N}}}(i) - \vec{h}_{\boldsymbol{\mathcal{N}}}(j)\right) \end{cases}, \tag{27}$$

which by Props. 3.4 and 3.5 we see it is never proportional to $\vec{a}$, given $gcd(\vec{a}) = 1$ and $\vec{n} \prec \vec{a}$ or $\vec{n} \not\preceq \vec{a}$. If it happens that it is zero, then no information can be obtained. This concludes the proof by noticing there is no way to construct any state achieving privacy for the function presented. □

In this proof, the tools and approach used provide a good insight on how to deal with the other cases. We present another statement for the *Minimal privacy zone*, for which a similar proof can be found in Appendix F.

Theorem 3.4 (Minimal privacy zone)**.** *Let $\vec{a}, \vec{n} \in \mathbb{Z}^k$, $gcd(\vec{a}) = 1$ and $f(\boldsymbol{\theta})$ be the linear function given by $f(\boldsymbol{\theta}) = \vec{a}\cdot\vec{\boldsymbol{\theta}}$. Then, there is only one family of pure states that is capable of estimating privately the function f using $\vec{n} = \vec{a}$ distributed resources and access to local separable dynamics $U_{\boldsymbol{\theta}}$.*

$$F_{GHZ} = \{\alpha \left|0\right\rangle^{\otimes n} + \beta \left|1\right\rangle^{\otimes n} : \alpha, \beta \in \mathbb{C} \setminus \{0\}, |\alpha|^2 + |\beta|^2 = 1\}$$

$$\mathcal{P}(\mathcal{Q}(U_{\boldsymbol{\theta}} \left|\psi\right\rangle), \vec{a}) = 1 \quad \iff \quad \exists U \in LU : U \left|\psi\right\rangle \in F_{GHZ}$$

Thms. 3.3 and 3.4 allow us to define the minimum amount of distributed resources so we can have a private state for a target linear function $f(\vec{\boldsymbol{\theta}}) = \vec{a}\cdot\vec{\boldsymbol{\theta}}$. This minimum is provided by the vector $\vec{a}$, under the separable Hamiltonians and integer target functions assumptions.

Finally, one can also wonder what happens if we add more qubits than we need, but not sufficient enough, for example, to build two copies of a GHZ state with $\vec{a}$ resources. In order to do so, let us first provide an example of a simple transformation that preserves privacy:

Example 3.2. *Suppose we have a partition for the distributed qubits given by $\boldsymbol{\mathcal{N}}$ with corresponding vector of resources $\vec{n} = (2, 1, 2)$ and we are trying to estimate a function $\vec{a} = (1, 1, 1) \prec \vec{n}$. If one uses dynamics generated by Z operators, one can simply take a GHZ state and add ancillas in a separable way:*

$$\begin{aligned} \left|\psi\right\rangle &= \frac{1}{\sqrt{2}}\left(\left|\overbrace{\underbrace{0}_{a_1}\underbrace{0}_{b_1}}^{n_1}\overbrace{\underbrace{0}_{a_2}\underbrace{0}_{b_2}}^{n_2}\overbrace{\underbrace{0}_{a_3}\underbrace{0}_{b_3}}^{n_3}\right\rangle + \left|\overbrace{\underbrace{1}_{a_1}\underbrace{0}_{b_1}}^{n_1}\overbrace{\underbrace{1}_{a_2}\underbrace{1}_{b_2}}^{n_2}\overbrace{\underbrace{0}_{a_3}\underbrace{0}_{b_3}}^{n_3}\right\rangle\right), \\ &= \frac{1}{\sqrt{2}}\left(\left|0_{a_1}0_{a_2}0_{a_3}\right\rangle + \left|1_{a_1}1_{a_2}1_{a_3}\right\rangle\right)\left|0_{b_1}0_{b_3}\right\rangle. \end{aligned} \tag{28}$$

This state is still private. And more so, it is still private if one chooses any state for the ancillas over the possible bit strings for the qubits $\vec{b} = \vec{n} - \vec{a}$, meaning $(0_{b_1}0_{b_3}), (0_{b_1}1_{b_3}), (1_{b_1}0_{b_3})$,

$(1_{b_1}1_{b_3})$. *Additionally, if one does any superposition of local permutations in* $S_{\boldsymbol{\mathcal{N}}}$ *over the qubits, this action preserves the vectorial Hamming-weight, meaning it will also preserve the privacy.*

Taking this example, let us formalize everything by introducing some families of pure states that emerge as a natural consequence of the equivalence of the vectorial Hamming weight under local permutations of qubits:

Definition 3.5 (Distributed s-States)**.** *Let* $\boldsymbol{\mathcal{N}} = \{\mathcal{N}_\mu\}_{\mu=1,\dots,k}$ *be a partition of the set of qubits and* $s \in \mathbb{F}_2^n$ *be a bit string. We call a quantum state* $|\psi\rangle$ *a distributed* s*-state if it can be represented by:*

$$|\psi\rangle = \sum_{r\in[s]_{\boldsymbol{\mathcal{N}}}} \alpha_r |r\rangle ,$$

where $\alpha_r \in \mathbb{C}$*, such that* $\sum_r |\alpha_r|^2 = 1$ *for normalization purposes. Let* $\vec{s} = \vec{h}_{\boldsymbol{\mathcal{N}}}(s)$*, we denote this family of states by* $\mathcal{D}(\boldsymbol{\mathcal{N}}, \vec{s})$*.*

Note that the bit strings that belong to the equivalence class $[s]_{\boldsymbol{\mathcal{N}}}$ are exactly the ones for which the vectorial Hamming weight $h_{\boldsymbol{\mathcal{N}}}$ is the same, as they all differ by a permutation in $S_{\boldsymbol{\mathcal{N}}}$ from each other. In particular, if it was the case that the partitions have size 1 ($k = 1$) and α_r is the same for every r, one would recover the regular Dicke state with $|\mathcal{N}_1| = n$ qubits and $h(s) = m$ excitations ($|D_n^m\rangle$).

This allows us to define a countable number of families that achieves privacy at estimating a linear function:

Definition 3.6 ($\vec{a}$-Private-Ancilla States)**.** *Let* $\boldsymbol{\mathcal{N}} = \{\mathcal{N}_\mu\}_{\mu=1,\dots,k}$ *correspond to the partition of a set of distributed qubits, with associated resource vector* $\vec{n} \succeq \vec{a}$ *necessarily.*

$$\mathcal{F}(\boldsymbol{\mathcal{N}}, \vec{a}, \vec{d}) = \Big\{ \alpha |\psi\rangle + \beta |\tilde{\psi}\rangle , |\psi\rangle \in \mathcal{D}(\boldsymbol{\mathcal{N}}, \vec{d}), |\tilde{\psi}\rangle \in \mathcal{D}(\boldsymbol{\mathcal{N}}, \vec{a} + \vec{d}), \\ \alpha, \beta \in \mathbb{C} \setminus \{0\}, |\alpha|^2 + |\beta|^2 = 1 \Big\}, \quad (29)$$

where $\vec{d}$ *can be such that* $\vec{d} \in \mathbb{N}_0^k, \vec{0} \preceq \vec{d} \preceq \vec{n} - \vec{a}$*. Note that for a fixed* $\vec{a}$ *there will be multiple* $\vec{d}$ *available, depending on the number of qubits. Each of them defines one family of private states.*

To provide some intuition, let us provide all the private families for a given set of resources and target function:

Example 3.3. *Let* $\vec{n} = (2, 2, 5)$ *and* $\vec{a} = (1, 2, 3)$*. This implies we have additionally in each node* $\vec{b} = (1, 0, 2)$ *distributed qubits. However, we can attribute to the ancilla qubits different strings* s *such that* $\vec{h}_{\boldsymbol{\mathcal{N}}}(s) = \vec{b}_1$ *defining different families of private states. One way to see this is considering that* $\vec{b}_1$ *represents the amount of 1's we put in our ancilla qubits. We can additionally define a vector* $\vec{b}_0$ *as the amount of 0's in the ancilla qubits. Naturally* $\vec{b}_0 + \vec{b}_1 = \vec{b}$*. The total amount of 6 families are given by:*

$$\begin{aligned}
s_1 &= 0_{a_1}0_{b_1}\ 00_{a_2}\ 000_{a_3}00_{b_3}, & \tilde{s}_1 &= 1_{a_1}0_{b_1}\ 11_{a_2}\ 111_{a_3}00_{b_3}, & \vec{d}_1 &= (0,0,0)\\
s_2 &= 0_{a_1}0_{b_1}\ 00_{a_2}\ 000_{a_3}10_{b_3}, & \tilde{s}_2 &= 1_{a_1}0_{b_1}\ 11_{a_2}\ 111_{a_3}10_{b_3}, & \vec{d}_2 &= (0,0,1)\\
s_3 &= 0_{a_1}0_{b_1}\ 00_{a_2}\ 000_{a_3}11_{b_3}, & \tilde{s}_3 &= 1_{a_1}0_{b_1}\ 11_{a_2}\ 111_{a_3}11_{b_3}, & \vec{d}_3 &= (0,0,2)\\
s_4 &= 0_{a_1}1_{b_1}\ 00_{a_2}\ 000_{a_3}00_{b_3}, & \tilde{s}_4 &= 1_{a_1}1_{b_1}\ 11_{a_2}\ 111_{a_3}00_{b_3}, & \vec{d}_4 &= (1,0,0)\\
s_5 &= 0_{a_1}1_{b_1}\ 00_{a_2}\ 000_{a_3}10_{b_3}, & \tilde{s}_5 &= 1_{a_1}1_{b_1}\ 11_{a_2}\ 111_{a_3}10_{b_3}, & \vec{d}_5 &= (1,0,1)\\
s_6 &= 0_{a_1}1_{b_1}\ 00_{a_2}\ 000_{a_3}11_{b_3}, & \tilde{s}_6 &= 1_{a_1}1_{b_1}\ 11_{a_2}\ 111_{a_3}11_{b_3}, & \vec{d}_6 &= (1,0,2)
\end{aligned}$$

$$\mathcal{F}(\boldsymbol{\mathcal{N}},\vec{a},\vec{d_i}) = \Big\{\alpha \sum_{r\in[s_i]_{\boldsymbol{\mathcal{N}}}} \alpha_r \left|r\right\rangle + \beta \sum_{\tilde{r}\in[\tilde{s}_i]_{\boldsymbol{\mathcal{N}}}} \alpha_{\tilde{r}} \left|\tilde{r}\right\rangle, \alpha,\beta\in\mathbb{C}\setminus\{0\}, |\alpha|^2+|\beta|^2=1\Big\}.$$

Which is equivalent to saying:

$$\mathcal{F}(\boldsymbol{\mathcal{N}},\vec{a},\vec{d_i}) = \Big\{\alpha\left|\psi\right\rangle + \beta\left|\tilde{\psi}\right\rangle, \left|\psi\right\rangle\in\mathcal{D}(\boldsymbol{\mathcal{N}},s_i), \left|\tilde{\psi}\right\rangle\in\mathcal{D}(\boldsymbol{\mathcal{N}},\tilde{s}_i), \\ \alpha,\beta\in\mathbb{C}\setminus\{0\}, |\alpha|^2+|\beta|^2=1\Big\}.$$

The number of existent families of states depends on the number of ancilla qubits in each node and the different ways one can prepare these ancillas. Considering that a node μ has n_μ qubits and is trying to estimate the linear function with correspondent a_μ, then one has $b_\mu = n_\mu - a_\mu$ ancilla qubits. This means we have $b_\mu + 1$ ways to find bitstrings with different Hamming-weights. The overall number of families is given by $\prod_{\mu\in V}(b_\mu+1)$. By construction, all the states that fit within one of these families are private for the estimation of $f(\boldsymbol{\theta}) = \vec{a}\cdot\vec{\boldsymbol{\theta}}$:

Proposition 3.7. *All families of pure states $\mathcal{F}(\boldsymbol{\mathcal{N}},\vec{a},\vec{d})$, are capable of estimating privately the function $f(\boldsymbol{\theta}) = \vec{a}\cdot\vec{\boldsymbol{\theta}}$ using $\vec{n} = \vec{a}+\vec{b}$ distributed resources.*

This allows us to finally get to the statement on privacy for when the amount of resources is larger than the minimum needed, but not as large so one could have multiples of the number of resources.

Theorem 3.5 (Minimal Plus Ancilla Zone)**.** *Let $\vec{a},\vec{b},\vec{n}\in\mathbb{Z}^k$, $gcd(\vec{a}) = 1$ and $f(\boldsymbol{\theta})$ be the linear function given by $f(\boldsymbol{\theta}) = \vec{a}\cdot\vec{\boldsymbol{\theta}}$. Then, all pure states, up to LU, capable of estimating privately the function f using $\vec{n} = \vec{a}+\vec{b}$ distributed resources and access to local separable dynamics $U_{\boldsymbol{\theta}}$, belong a family of the set of $\vec{a}$-Private-Ancilla States introduced in Def. 3.6.*

$$\mathcal{P}(\mathcal{Q}(U_{\boldsymbol{\theta}}\left|\psi\right\rangle),\vec{a}) = 1 \quad\Longleftrightarrow\quad \exists U\in LU, \vec{d}\in\mathbb{N}_0^k, \vec{0}\preceq\vec{d}\preceq\vec{n}-\vec{a} : U\left|\psi\right\rangle\in\mathcal{F}(\boldsymbol{\mathcal{N}},\vec{a},\vec{d})$$

The proofs for the above two statements, Prop. 3.7 and Thm. 3.5 are provided over Appendix F, following similar arguments as the proof for Thm. 3.3. Moreover, one can find an expression for QFI of the private state very similar to the one for the GHZ state, as detailed in the proof of Prop. 3.7.

Finally, we can discuss the case where we have multiples of the number of resources. For this case, we will not provide a complete set of private states, in the sense we will not prove that the states built in such fashion are the only private states. However, we are able to prove that every state built as so is indeed private. The way to think of this case is to consider that we have logical qubits such that the encoding dynamics by default already encode the desired function. This means exactly choosing our logical qubits to be the ones such that $\alpha\left|0_L\right\rangle + \beta\left|1_L\right\rangle$ generates a private state:

$$\begin{aligned} \left|0_L\right\rangle &\in \mathcal{D}(\boldsymbol{\mathcal{N}},\vec{d}), \\ \left|1_L\right\rangle &\in \mathcal{D}(\boldsymbol{\mathcal{N}},\vec{a}+\vec{d}), \end{aligned} \tag{30}$$

for some $\vec{d}$, using the notation introduced in Defs. 3.5,3.6. Using for each logical qubit $\vec{a}+\vec{b}$ resources, encompasses the case of $\vec{b} = \vec{0}$ which is the single GHZ state distributed among the $\vec{a}$ resources, and the states in Minimal plus ancilla region. Using these states, and our regular estimation scenario of $(\rho, U_{\boldsymbol{\theta}}, \vec{a}\cdot\vec{\boldsymbol{\theta}})$ it is easy to understand that now our dynamics when applied to a superposition of $\left|0_L\right\rangle$ and $\left|1_L\right\rangle$ will always be sensitive only to the desired function $f(\boldsymbol{\theta}) = \vec{a}\cdot\vec{\boldsymbol{\theta}}$. Moreover, not all logical qubits need to be defined in the same way, as long as each of them are private. Let us define the states which are built like this:

Definition 3.7 (Private Logical States)**.** *Let* $\mathfrak{N} = \{\boldsymbol{\mathcal{N}}_1, \boldsymbol{\mathcal{N}}_2, \cdots, \boldsymbol{\mathcal{N}}_d\}$ *be a set of partitions such that each* $\boldsymbol{\mathcal{N}}_l$ *defines the partition set of a private state, with associated vector of resources* $\vec{n}_l = \vec{a} + \vec{b}_l \succeq \vec{a}\ \forall l$*. For each partition, one can define two logical states, such that:*

$$|0_L\rangle_l \in \mathcal{D}(\boldsymbol{\mathcal{N}}_l, \vec{d}_l),$$
$$|1_L\rangle_l \in \mathcal{D}(\boldsymbol{\mathcal{N}}_l, \vec{a} + \vec{d}_l).$$

The set of logical private states can be defined as follows:

$$\mathfrak{F} = \left\{ |\psi\rangle = \sum_{j=0}^{2^d-1} \alpha_j \, |j_1 j_2 \cdots j_d\rangle : \alpha_j \in \mathbb{C}, |j_l\rangle \in \{|0_L\rangle_l, |1_L\rangle_l\}, \langle\psi|\psi\rangle = 1 \right\}.$$

As one can see, the problem is now combinatorial. One can arrange the qubits in multiple partitions, and pick multiple private logical states inside of these partitions. Let us make a statement about the privacy of states built like this, which we prove in Appendix F:

Theorem 3.6 (Multiple Privacy)**.** *All states which are described as a private logical state (Def. 3.7) define private states for quantum distributed sensing, up to LU operations.*

This has an important consequence: we can treat this case as the single-parameter scenario. In particular, one could use the robustness results of the single-parameter case and construct equivalent states, but instead using the logical qubits. Moreover, we can use results on how logical qubits are affected by error to predict how a state made of those logical qubits evolves under error.

This section finishes with a set of private states for distributed quantum sensing with separable dynamics, and proof that, for limited resources, they constitute the only set of private states. If we extend our resources, we find a construction of sets of private states, by logically encoding multiple qubits into logical qubits that are only sensitive to our target function.

3.4 Privacy for Arbitrary States with General Hamiltonians

In a similar manner as for separable hamiltonians, the problem complexity can be reduced by choosing an appropriate basis. The basis we will use in this case will be the basis introduced in Eq. 10, constituted by the eigenvectors of the Hamiltonian. This already implies that finding a private state requires finding eigenstates of the Hamiltonian, which is not necessarily trivial as it was for the separable Hamiltonian scenario. By choosing this basis one can build a very similar system to Eq. 68 in the following way:

$$\begin{aligned}
\mathcal{Q}_{\mu\nu}(\rho_{\boldsymbol{\theta}}) &= 4\mathrm{Re}\left\{ \sum_{\vec{l},\vec{m}} \alpha^*_{\vec{l}}\alpha_{\vec{m}} \langle\lambda_{\vec{l}}|\boldsymbol{H}_\mu \boldsymbol{H}_\nu|\lambda_{\vec{m}}\rangle - \sum_{\vec{l},\vec{m}} \alpha^*_{\vec{l}}\alpha_{\vec{m}} \langle\lambda_{\vec{l}}|\boldsymbol{H}_\mu|\lambda_{\vec{m}}\rangle \sum_{\vec{p},\vec{q}} \alpha^*_{\vec{p}}\alpha_{\vec{q}} \langle\lambda_{\vec{p}}|\boldsymbol{H}_\nu|\lambda_{\vec{q}}\rangle \right\} \\
&= 4\mathrm{Re}\left\{ \sum_{\vec{l},\vec{m}} \alpha^*_{\vec{l}}\alpha_{\vec{m}} \lambda^\mu_{l_\mu}\lambda^\nu_{m_\nu} \langle\lambda_{\vec{l}}|\lambda_{\vec{m}}\rangle - \sum_{\vec{l},\vec{m}} \alpha^*_{\vec{l}}\alpha_{\vec{m}} \lambda^\mu_{m_\mu} \langle\lambda_{\vec{l}}|\lambda_{\vec{m}}\rangle \sum_{\vec{p},\vec{q}} \alpha^*_{\vec{p}}\alpha_{\vec{q}} \lambda^\nu_{q_\nu} \langle\lambda_{\vec{p}}|\lambda_{\vec{q}}\rangle \right\} \\
&= 4\sum_{\vec{m}} |\alpha_{\vec{m}}|^2 \lambda^\mu_{m_\mu}\lambda^\nu_{m_\nu} - \sum_{\vec{m}} |\alpha_{\vec{m}}|^2 \lambda^\mu_{m_\mu} \sum_{\vec{q}} |\alpha_{\vec{q}}|^2 \lambda^\nu_{q_\nu} \\
\boldsymbol{\mathcal{Q}}(\rho_{\boldsymbol{\theta}}) &= C\mathfrak{Q}C^T,
\end{aligned} \tag{31}$$

where we used the fact that the basis states are $|\lambda_{\vec{j}}\rangle$ with $\vec{j}$ being given by some labeling function in a space with dimension of the product of the local Hilbert spaces, *e.g.* $\vec{j} \in \{0, \cdots, |\mathcal{H}_1|\} \times \cdots \times \{0, \cdots, |\mathcal{H}_k|\}$. In this case, for each of the vectors $\vec{j}$ with associated $\alpha_{\vec{j}}$ in $\mathfrak{Q}$, there will exist an associated $c_{\vec{j}}$ in C, given by $c_{\vec{j}} = (\lambda^1_{j_1}, \lambda^2_{j_2}, \cdots, \lambda^k_{j_k}) \in \mathcal{O}$. We provide a simple example:

Example 3.4. *Let $k = 3$ meaning 3 nodes, each holding one qubit and having access to a Z hamiltonian (the local dynamics are given by $U_{\theta_\mu} = e^{-i\theta_\mu Z}$). Each local set of eigenvalues is the same, $\{-1, +1\}$, meaning $\mathcal{O} = \{-1, +1\} \times \{-1, +1\} \times \{-1, +1\}$. The set of possible eigenstates of the distributed Hamiltonian are then $|j_1 j_2 j_3\rangle$ where $|j_i\rangle \in \{|0\rangle, |1\rangle\}$. The possible set of functions can be mapped to $c_{\vec{j}} = ((-1)^{j_1}, (-1)^{j_2}, (-1)^{j_3})$. They form the vertices of a cube centered in 0 with side equal to 2.*

Note that the matrix $\mathfrak{Q}$ can be written again in the same form as before, with a slight change: $\mathfrak{Q} = \text{diag}(\vec{\alpha}) - \vec{\alpha}\vec{\alpha}^T = \Lambda - \vec{\alpha}\vec{\alpha}^T$, where we used that each entry of $\vec{\alpha}$ corresponds to the probability amplitude $|\alpha_{\vec{j}}|^2$ for each and every $\vec{j}$. This vector will have the length of the amount of vectors $\vec{j}$ there are, *i.e.* the total Hilbert space dimension. Given Thm. E.1, we know this matrix has rank equal to rank $\Lambda - 1$.

From here we can already make some statements about finding private states, although we cannot go very far as it highly depends on the structure of $\mathcal{O}$, which naturally depends on the Hamiltonian. In order to better analyze this let us introduce the set of vectors going from each point of $\mathcal{O}$ to another, as it will become apparent later that these are the vectors defining linear functions for which we can find private states.

Definition 3.8. *Let $\mathcal{O}$ be a discrete subset inside an orthotope in k dimensions over some ordered ring $\mathbb{K}$. Define the higher order discrete subset $\mathcal{O}^2_\pm$ as:*

$$\mathcal{O}^2_\pm = \{\vec{z} \in \mathbb{K}^k : \vec{z} = \vec{x} \pm \vec{y}, \forall \vec{x}, \vec{y} \in \mathcal{O}\}. \tag{32}$$

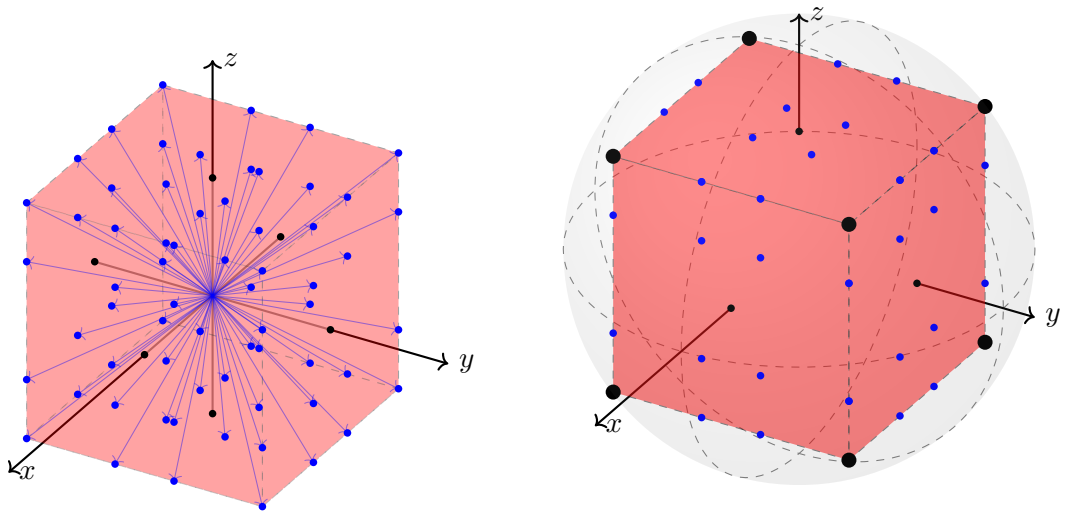
One can further extend the class of equivalence of linear functions to a class of equivalence of the discrete subset of the orthotopes. As before $f(\boldsymbol{\theta}) \sim g(\boldsymbol{\theta})$ if $\exists \alpha \in \mathbb{R} : f(\boldsymbol{\theta}) = \alpha g(\boldsymbol{\theta})$, one can say two sets of vectors are equivalent $\mathcal{O}_1 \sim \mathcal{O}_2$ if $\forall \vec{v} \in \mathcal{O}_1 \exists \alpha \in \mathbb{R}, \vec{w} \in \mathcal{O}_2 : \vec{v} = \alpha \vec{w}$ and the correspondence is bijective. We say one subset contains another up to equivalence $\mathcal{O}_1 \lesssim \mathcal{O}_2$ if $\mathcal{O}_1 \sim \tilde{\mathcal{O}}_1 \subseteq \mathcal{O}_2$. Using this, we can perform a statement on a necessary condition in order to create private state in this scenario:

Theorem 3.7 (Existence of Private States)**.** *Let a distributed sensing scenario be governed by local encoding dynamics in the form of Eq. 7, with associated discrete subset $\mathcal{O}$. For each vector $\vec{a}$ belonging to the higher order discrete subset $\mathcal{O}^2_-$, one can find a private state with respect to the linear function $f(\boldsymbol{\theta}) = \vec{a} \cdot \vec{\boldsymbol{\theta}}$. Moreover, no vector outside the equivalence class of $\mathcal{O}^2_-$ has a private state.*

Let us provide again another more complex example to help visualize what we are doing, by plotting an illustration of the functions such that a private state exists.

Example 3.5. ***(Cube in 3-D)*** *Let the three local hamiltonians $\{H_1, H_2, H_3\}$ have possible eigenvalues $\{\lambda^\mu_j\}^{\mu=1,2,3}_{j=1,\ldots,|H_\mu|}$. All of the vectors in blue with accompanying points correspond to the discrete subset $\mathcal{O}$ and correspond to all the possible combinations of the eigenvalues in each local hamiltonian $(\lambda^1_i, \lambda^2_j, \lambda^3_k)$. These are the private linear functions one has access to, since for each of them we prove the existence of a private state. The 3-cube in red (given that the dimension $k = 3$) corresponds to the $3-$orthotope $\overline{\mathcal{O}}$. The blue and black dots on the right side correspond to the set of $\mathcal{O} \cap \overline{\mathcal{O}}$. The black dots on the right side*

also correspond to the vertices of the orthotope $V(\overline{\mathcal{O}})$, which can be seen as the intersection with the k-sphere. These correspond to the maximum of the 2-norm of the vectors inside the orthotope.



Moreover, one may wonder about the possibility of finding private states for functions within $\mathcal{O}$, not only in $\mathcal{O}^2_-$. This is again highly dependent on the Hamiltonian. For this reason we will give a sufficient condition for one to find these Hamiltonians, which relates with the inclusion of $\mathcal{O}$ in the higher order subset $\mathcal{O}^2_-$:

Proposition 3.8. *Let $\{\boldsymbol{H}_\mu\}_{\mu\in V}$ be the Hamiltonians describing some local general encoding dynamics.*

$$\forall\ \mu \in V\ \exists\ X_\mu \in \mathbb{1}\otimes\mathcal{P}_\mu : \{X_\mu, \boldsymbol{H}_\mu\} = 0 \implies \mathcal{O} \subsetneq \mathcal{O}^2_- \tag{33}$$

Where $\mathbb{1}\otimes\mathcal{P}_\mu$ are the Pauli strings where only the elements in μ can be non-identity. This means the functions in $\mathcal{O}$ are available privately by choosing an appropriate state.

We prove Thm. 3.7 and Prop. 3.8 in Appendix G. The latter is supposed to give some symmetry conditions for the Hamiltonian, under which the functions available are directly extractable from the original set $\mathcal{O}$. Note that the form of $\mathcal{O}$ is not always a cube centered in the origin, even though $\mathcal{O}^2_-$ is. Prop. 3.8 also implies that $\mathcal{O}$ will be symmetric with respect to the origin. From here, one can deduce a simple, yet important consequence that relates with the idea of concentration of information.

Corollary 3.1 (Information Concentration)**.** *Given a distributed sensing scenario governed by local encoding dynamics in the form of Eq. 7, the maximum information extractable, given by functions of parameters in the vertices of $\overline{\mathcal{O}}^2_-$, is accessible only by a private state.*

The proof for Corol. 3.1 can also be found over Appendix G. This has important consequences, and provides an intuition that has been in the background the whole time: one can either try and estimate one function with maximum precision, or a set of functions with less precision each. Moreover, one can retrieve the solutions for separable Hamiltonians from Thm. 3.7, by looking at the imposed condition on $gcd(\vec{a}) = 1$. Taking into consideration that the orthotope $\mathcal{O} \subseteq \mathbb{Z}^k$, the existence of private states is a consequence of integers' properties.

4 Robustness

So far, we have been able to calculate the QFI for special types of quantum states. We started with the case of stabilizer states with separable Hamiltonians. We then generalized for any arbitrary pure state, still under the assumption of separable Hamiltonians. We then lifted this last assumption to general local Hamiltonians, at the expense of not being able to identify the state, and instead proving that private states still exist and for which functions they do exist. The next logical step is to consider mixed states as well. These types of states are often associated with the presence of noise in the state, hence the name of this section. Robustness should measure the ability of a quantum state to retain some of its properties upon being affected by noise [55, 57–59]. In our case, our goal is to maximize precision, which is connected with the maximization of the QFI. Robustness is then linked to how the QFI varies as noise is applied onto the system. In this section, we will start by finding a way to calculate the QFI of mixed states and verify how the QFI changes under different noises types, keeping in mind the privacy as well. Moreover, we assume that the noise is applied to the state prior to any encoding dynamics, as this noise should be the one that could possibly break privacy.

4.1 QFI for Mixed States

Starting with the equation for the QFI in the multiparameter scenario:

$$\mathcal{Q}_{\mu\nu}(\rho_{\boldsymbol{\theta}}) = \operatorname{Tr} \mathcal{R}^{-1}_{\rho_{\boldsymbol{\theta}}}(\partial_{\theta_\mu}\rho_{\boldsymbol{\theta}})\rho_{\boldsymbol{\theta}}\mathcal{R}^{-1}_{\rho_{\boldsymbol{\theta}}}(\partial_{\theta_\nu}\rho_{\boldsymbol{\theta}}), \tag{34}$$

where the super operator $\mathcal{R}^{-1}_{\rho_{\boldsymbol{\theta}}}(\hat{O})$ is the inverse of the super operator $\mathcal{R}_{\rho_{\boldsymbol{\theta}}}(\hat{O})$, defined by the following set of equations:

$$\begin{aligned} \mathcal{R}_{\rho}(O) &= \frac{\rho O + O\rho}{2}, \\ \mathcal{R}^{-1}_{\rho}(O) &= \sum_{j,k} \frac{2}{\lambda_j + \lambda_k} O_{jk} \left|\mathcal{G}_j\right\rangle\!\left\langle\mathcal{G}_k\right|. \end{aligned} \tag{35}$$

Given a decomposition of the density matrix in its eigenvectors $\rho = \sum_k \lambda_k \left|\mathcal{G}_k\right\rangle \left\langle\mathcal{G}_k\right|$ and the matrix elements $O_{jk} = \left\langle\mathcal{G}_j\right| \hat{O} \left|\mathcal{G}_k\right\rangle$. Developing Eq. 34, one can arrive at the following expression, similar to [60]:

$$\mathcal{Q}_{\mu\nu}(\rho_{\boldsymbol{\theta}}) = \sum_{\substack{n\in\text{supp} \\ k\in\text{supp}}} 2\frac{(\lambda_n - \lambda_k)^2}{\lambda_n + \lambda_k} \left\langle\mathcal{G}_n|\boldsymbol{G}_\mu|\mathcal{G}_k\right\rangle \left\langle\mathcal{G}_k|\boldsymbol{G}_\nu|\mathcal{G}_n\right\rangle + \sum_{\substack{n\in\text{null} \\ k\in\text{supp}}} 4\lambda_k \left\langle\mathcal{G}_n|\boldsymbol{G}_\mu|\mathcal{G}_k\right\rangle \left\langle\mathcal{G}_k|\boldsymbol{G}_\nu|\mathcal{G}_n\right\rangle, \tag{36}$$

where we used supp and to denote the indices k such that λ_k is either positive or zero. This can be further simplified when $\rho = \sum_k \lambda_k \left|\mathcal{G}_k\right\rangle \left\langle\mathcal{G}_k\right|$ is given in an orthonormal basis, *i.e.* such that every $\left\langle\mathcal{G}_j|\mathcal{G}_k\right\rangle = \delta_{jk}$. Even if this is not the case, it is a well established property of quantum information that one can always find a basis for $\left|\mathcal{G}_j\right\rangle$ that makes a certain density operator have such form. Nonetheless, one arrives at:

$$\mathcal{Q}_{\mu\nu}(\rho_{\boldsymbol{\theta}}) = \sum_{\substack{n>k\in\text{supp} \\ n\neq k}} 4\left[\frac{(\lambda_n - \lambda_k)^2}{\lambda_n + \lambda_k} - (\lambda_n + \lambda_k)\right] \operatorname{Re}\left\{a^\mu_{nk} a^\nu_{kn}\right\} + \sum_{n\in\text{supp}} \lambda_n \mathcal{Q}_{\nu\mu}(\left|\mathcal{G}_n\right\rangle), \tag{37}$$

where $a^\mu_{nk} = \left\langle\mathcal{G}_n|\boldsymbol{G}_\mu|\mathcal{G}_k\right\rangle$. The entire derivation of these equations can be found in Appendix H. In the following sections we will assume that the encoding dynamics are generated by Z operators, without loosing generality. If they are generated by other generator

G, assume that dephasing noise is given by an equivalent quantum channel that has a mixture of error in the direction of G. For the bit-flip noise, assume the error is in the direction of some $G^{\perp}$. Again, we also assume that the noise is applied to the state, prior to evolution under the dynamics that encode the parameters $\boldsymbol{\theta}$.

4.2 Dephasing Noise

Dephasing noise is characterized by applying a quantum channel with a certain probability of a Z error. Taking a GHZ state with $\vec{n}$ qubits distributed over the network, the usual encoding dynamics in the Z direction and the usual target function $f(\boldsymbol{\theta}) = \vec{a}\cdot\vec{\boldsymbol{\theta}}$, such that $\vec{a} = \vec{n}$, *i.e.* we are working with a perfectly private state. Since the GHZ state is made up of eigenvectors of the Z operator, dephasing noise acts identically on whichever qubit of the GHZ state. Namely consider the two orthogonal states, differeing from applying one Z operation on whichever qubit, $|GHZ^{\pm}\rangle = 1/\sqrt{2}(|0\rangle^{\otimes n} \pm |1\rangle^{\otimes n}) \equiv |\mathcal{G}_0^{\pm}\rangle$, where $n = \|\vec{n}\|_1$. Applying a dephasing noise channel to a $|GHZ^{\pm}\rangle$ results in introducing a mixture between these two states:

$$\mathcal{D}_i(\rho, p) = (1-p)\rho + pZ_i\rho Z_i, \qquad Z\,|\mathcal{G}_0^{\pm}\rangle = |\mathcal{G}_0^{\mp}\rangle\,. \tag{38}$$

Applying this recursively for each qubit, we can find the following expression for an initial GHZ state :

$$\begin{aligned} \mathfrak{D}(\rho, \vec{p}) &= \mathcal{D}_1^{p_1} \circ \mathcal{D}_2^{p_2} \circ \cdots \circ \mathcal{D}_n^{p_n}(\rho), \\ \mathfrak{D}(|\mathcal{G}_0^{\pm}\rangle\langle\mathcal{G}_0^{\pm}|\,, \vec{p}) &= E(\vec{p})\,|\mathcal{G}_0^{\pm}\rangle\langle\mathcal{G}_0^{\pm}| + O(\vec{p})\,|\mathcal{G}_0^{\mp}\rangle\langle\mathcal{G}_0^{\mp}|\,, \end{aligned} \tag{39}$$

where the even, $E(\cdot)$, and ddd functions, $O(\cdot)$, correspond to the Kraus operators of the total channel with even and odd number of Z operators, and were introduced in [61] to calculate the fidelity of a GHZ state. One can use Eq. 36 to calculate the QFI of a mixed state where we have a mixture between $|\mathcal{G}_0^{\pm}\rangle$, given by $\rho = \lambda_+\,|\mathcal{G}_0^{+}\rangle\langle\mathcal{G}_0^{+}| + \lambda_-\,|\mathcal{G}_0^{-}\rangle\langle\mathcal{G}_0^{-}|$. Moreover, using the Z dynamics as $U_{\boldsymbol{\theta}} = \otimes_\mu\, e^{i\theta_\mu \sum_{j\in\mu} Z_j} = \otimes_\mu\, e^{i\theta_\mu \boldsymbol{Z}_\mu}$:

$$\begin{aligned} \mathcal{Q}_{\mu\nu}(\rho_{\boldsymbol{\theta}}) &= 4\frac{(\lambda_+ - \lambda_-)^2}{\lambda_+ + \lambda_-}\,\langle\mathcal{G}_0^{+}|\boldsymbol{Z}_\mu|\mathcal{G}_0^{-}\rangle\,\langle\mathcal{G}_0^{-}|\boldsymbol{Z}_\nu|\mathcal{G}_0^{+}\rangle \\ &= 4(\lambda_+ - \lambda_-)^2 a_\mu a_\nu, \end{aligned} \tag{40}$$

which preserves the privacy. This is a consequence of the dynamics being generated by the same operation as the error, namely by Z operators on each qubit. Moreover, if $\vec{p}$ is uniform, as in every qubit dephases at the same rate, we get that $\lambda_+ - \lambda_- = (1-2p)^n$, where n is the number of qubits suffering dephasing.

4.3 Bit-flip Noise

Bit-flip noise on the other hand is characterized by applying a quantum channel with a certain probability of X error. Under the same estimation scenario as before, we will arrive at the following density matrix:

$$\rho = \lambda_0\,|\mathcal{G}_0^{+}\rangle\langle\mathcal{G}_0^{+}| + \sum_{i=1}^{2^{n-1}-1} \lambda_i\,|\mathcal{G}_i^{+}\rangle\langle\mathcal{G}_i^{+}|\,, \tag{41}$$

where $|\mathcal{G}_m\rangle = 1/\sqrt{2}(|m\rangle + |\overline{m}\rangle)$ and $0 \le m \le 2^{(n-1)} - 1$ to prevent repetition of states, given the invariance of $m \to \overline{m}$. Taking the derivation of the QFI in Eq. 37 we get that

all terms a^{μ}_{nk} are going to be zero cause the dynamics are generated by Z operators, and the errors are generated by X operators. This way, no operator containing only $\{\mathbb{1}, Z\}$ terms will ever take one $|\mathcal{G}_j\rangle$ to another $|\mathcal{G}_k\rangle$, since this map is generated by some operator containing only $\{\mathbb{1}, X\}$ terms. This results in the QFI being given by:

$$\begin{aligned} \boldsymbol{\mathcal{Q}}(\rho_{\boldsymbol{\theta}}) &= 4 \sum_{j=0}^{2^{n-1}-1} \lambda_j \vec{h}^*_{\boldsymbol{\mathcal{N}}}(j) \vec{h}^*_{\boldsymbol{\mathcal{N}}}(j)^T, \\ \lambda_j &= g(\vec{p}, j) + g(\vec{p}, \bar{j}), \end{aligned} \tag{42}$$

where we introduce the function that maps a vector of reals and a bitstring into a real number, namely:

$$\begin{aligned} g : \mathbb{R}^k \times \mathbb{F}_2^k &\longrightarrow \mathbb{R} \\ g(\vec{p}, j) &\longmapsto \prod_{i=1}^{k} p_i^{j_i} (1 - p_i)^{1 - j_i}. \end{aligned} \tag{43}$$

One can observe in Eq. 42, complete privacy is lost as soon as one qubit suffers a bit-flip. This is due to the fact that now the generators of the dynamics are Z operators and the errors only contain X operators. However, one can still make a statement using the fifth property of the privacy measure: if the noise can be maintained under a certain threshold, then one can bound the loss of privacy. Equivalently, the amount of error will bound the amount of information leaked.

4.4 Depolarizing Noise

Depolarizing noise can be seen as a very symmetric noise, as it decoheres in every direction with identical probabilities. In particular, taking a GHZ state and applying a depolarizing channel in each qubit, one arrives at a state which is very similar to a generalized Werner state [62], apart from the identity not really being an identity matrix, but a diagonal matrix. Nonetheless, using the description of the depolarizing channel as in [61]:

$$\begin{aligned} \mathcal{D}_i^p(\rho) &= p\rho + \frac{1-p}{3} \left(X_i \rho X_i^\dagger + Y_i \rho Y_i^\dagger + Z_i \rho Z_i^\dagger \right) \\ &= \frac{1+2p}{3} \rho + \frac{2(1-p)}{3} \Lambda_i \left(Y_i \rho Y_i^\dagger \right). \end{aligned} \tag{44}$$

The density matrix can be expressed as:

$$\rho = \lambda_0^+ \left|\mathcal{G}_0^+\right\rangle\!\left\langle\mathcal{G}_0^+\right| + \lambda_0^- \left|\mathcal{G}_0^-\right\rangle\!\left\langle\mathcal{G}_0^-\right| + \sum_{i=1}^{2^n-2} \lambda_i \left|i\right\rangle\!\left\langle i\right|, \tag{45}$$

since $\langle i|j\rangle = \langle i|\mathcal{G}_0^{\pm}\rangle = 0$ for $i \neq 0, 2^n - 1$, and, similar to before, the dynamics are in Z, all the terms $a^{\mu}_{0^{\pm}j} = 0$. Moreover, the QFI of each of the $|i\rangle\langle i|$ with $i > 0$, is zero, as no information can be obtained from states which are just a binary string. This allows us to write the QFI matrix as:

$$\begin{aligned} \boldsymbol{\mathcal{Q}}(\rho_{\boldsymbol{\theta}}) &= 4 \frac{(\lambda_0^+ - \lambda_0^-)^2}{\lambda_0^+ + \lambda_0^-} \vec{a}\vec{a}^T + \sum_{j=1}^{2^n-2} \lambda_j \boldsymbol{\mathcal{Q}}(|j\rangle) \\ &= 4 \frac{(\lambda_0^+ - \lambda_0^-)^2}{\lambda_0^+ + \lambda_0^-} \vec{a}\vec{a}^T, \end{aligned} \tag{46}$$

where $\lambda_0^{\pm}$ can be found be solving the following set of equations:

$$\begin{cases} \lambda_0^+ + \lambda_0^- = g((1+2\vec{p})/3, 0) + g(2(1-\vec{p})/3, 0) \\ \lambda_0^+ - \lambda_0^- = g((4\vec{p}-1)/3, 0). \end{cases} \tag{47}$$

Importantly, this type of noise again preserves privacy. Unlike previous errors, this error contains both the same operators as in the encoding dynamics and orthogonal to the ones generating the dynamics. The privacy preservation in this case comes from the symmetry of this channel acting on the GHZ state, which is also highly symmetric.

4.5 Amplitude-Damping Noise

Amplitude-damping noise can be seen as a consequence of spontaneous emission of excited photons, in a way that the excited states (in our case $|1\rangle$), with some probability, p_i per qubit, go to the ground state (in our case $|0\rangle$). Taking a GHZ state and applying an amplitude-damping channel in each qubit, one arrives at something very similar to the depolarizing channel, with some slight changes:

$$\begin{aligned} \rho &= \lambda_0^+ |\mathcal{G}_0^+\rangle\langle\mathcal{G}_0^+| + \lambda_0^- |\mathcal{G}_0^-\rangle\langle\mathcal{G}_0^-| + \sum_{i=0}^{2^n-1} \lambda_i |i\rangle\langle i| \\ &= \lambda_0 |0\rangle\langle 0| + \lambda_0^+ |\mathcal{G}_0^+\rangle\langle\mathcal{G}_0^+| + \lambda_0^- |\mathcal{G}_0^-\rangle\langle\mathcal{G}_0^-| + \lambda_1 |1\rangle\langle 1| + \sum_{i=1}^{2^n-2} \lambda_i |i\rangle\langle i| . \end{aligned} \tag{48}$$

One can diagonalize the system into the following:

$$\rho = \tilde{\lambda}_0^+ |\tilde{\mathcal{G}}_0^+\rangle\langle\tilde{\mathcal{G}}_0^+| + \tilde{\lambda}_0^- |\tilde{\mathcal{G}}_0^-\rangle\langle\tilde{\mathcal{G}}_0^-| + \sum_{i=1}^{2^n-2} \lambda_i |i\rangle\langle i| . \tag{49}$$

The QFI can then be obtained by:

$$\boldsymbol{\mathcal{Q}}(\rho_{\boldsymbol{\theta}}) = 4\frac{(\tilde{\lambda}_0^+ - \tilde{\lambda}_0^-)^2}{\tilde{\lambda}_0^+ + \tilde{\lambda}_0^-} \left|\langle\tilde{\mathcal{G}}_0^+|Z|\tilde{\mathcal{G}}_0^-\rangle\right|^2 \vec{a}\vec{a}^T, \tag{50}$$

where $\tilde{\lambda}_0^{\pm}$ and $\tilde{\mathcal{G}}_0^{\pm}$ can be found from the solution of the following eigensystem, written in the basis $\{|0\rangle^{\otimes n} \equiv |0\rangle, |1\rangle^{\otimes n} \equiv |1\rangle\}$:

$$\begin{pmatrix} a & b \\ b & c \end{pmatrix} = \begin{pmatrix} 1 + \prod_i p_i & \prod_i \sqrt{1-p_i} \\ \prod_i \sqrt{1-p_i} & \prod_i (1-p_i) \end{pmatrix}. \tag{51}$$

Yet again, this noise still preserves privacy. The reason behind this comes again from the symmetric form of the GHZ state with respect to the Kraus operators of the amplitude damping channel, observed from Eq. 48.

4.6 Particle Loss

To check what happens to the state under particle loss, let us start with the simple case where we have $\vec{n} = \vec{a}$ resources. This means the only private state is given by the GHZ state, with the distribution of resources given by $\vec{a}$, in the regular setting. As it is known, the GHZ state has no resilience against particle loss, and all the information is lost upon particle loss. A GHZ state, $|\mathcal{G}_0^+\rangle$, after loosing whichever particle is transformed into:

$$\begin{aligned}\mathcal{E}_i(GHZ) &= \mathrm{Tr}_i\,|\mathcal{G}_0^+\rangle\langle\mathcal{G}_0^+| \\ &= \langle 0_i\,|\mathcal{G}_0^+\rangle\langle\mathcal{G}_0^+|\,0_i\rangle + \langle 1_i\,|\mathcal{G}_0^+\rangle\langle\mathcal{G}_0^+|\,1_i\rangle \\ &= \frac{1}{2}\left[|0_{\mathcal{N}\setminus i}\rangle\langle 0_{\mathcal{N}\setminus i}| + |1_{\mathcal{N}\setminus i}\rangle\langle 1_{\mathcal{N}\setminus i}|\right].\end{aligned} \tag{52}$$

Using again the equation for the noisy QFI, we get the QFI becomes 0 for whichever parameter, as this state is invariant under the encoding dynamics.

Throughout the paper, we have defined families of private states when we have more ancilla qubits at our disposal, besides the minimum amount to create a private state. One can observe that there are states in these private families that show robustness against particle loss. To do this, suppose we have a state belonging to one of these families, $\mathcal{F}(\boldsymbol{\mathcal{N}}, \vec{a}, \vec{d})$:

$$|\psi\rangle = \alpha\,|\psi_0\rangle + \beta\,|\psi_1\rangle\,, \qquad |\psi_0\rangle \in \mathcal{D}(\boldsymbol{\mathcal{N}}, \vec{d}), |\psi_1\rangle \in \mathcal{D}(\boldsymbol{\mathcal{N}}, \vec{a}+\vec{d}). \tag{53}$$

Let us first analyze what happens to the states in the private family $\mathcal{F}(\boldsymbol{\mathcal{N}}, \vec{a}, \vec{d})$ when a qubit is traced. Since we can choose whichever basis for the partial trace, let us measure the qubit j in the Z basis:

$$\begin{aligned}&|\psi_0\rangle \in \mathcal{D}(\boldsymbol{\mathcal{N}}, \vec{d}) \implies \langle 0_j|\psi_0\rangle \in \mathcal{D}(\boldsymbol{\mathcal{N}}\setminus j, \vec{d}), \\ &|\psi_1\rangle \in \mathcal{D}(\boldsymbol{\mathcal{N}}, \vec{a}+\vec{d}) \implies \langle 0_j|\psi_1\rangle \in \mathcal{D}(\boldsymbol{\mathcal{N}}\setminus j, \vec{a}+\vec{d}), \\ &\qquad\qquad \Downarrow \\ &\alpha'\,\langle 0_j|\psi_0\rangle + \beta'\,\langle 0_j|\psi_1\rangle \in \mathcal{F}(\boldsymbol{\mathcal{N}}\setminus j, \vec{a}, \vec{d}).\end{aligned} \tag{54}$$

This holds true if both $\langle 0_j|\psi_0\rangle$ and $\langle 0_j|\psi_1\rangle$ are larger then zero. If not, it will lead to a state with no information available. The same can be said if one measures the state $|\psi\rangle$ in $|1\rangle_j$:

$$\begin{aligned}&|\psi_0\rangle \in \mathcal{D}(\boldsymbol{\mathcal{N}}, \vec{d}) \implies \langle 1_j|\psi_0\rangle \in \mathcal{D}(\boldsymbol{\mathcal{N}}\setminus j, \vec{d}-\vec{e}_j), \\ &|\psi_1\rangle \in \mathcal{D}(\boldsymbol{\mathcal{N}}, \vec{a}+\vec{d}) \implies \langle 1_j|\psi_1\rangle \in \mathcal{D}(\boldsymbol{\mathcal{N}}\setminus j, \vec{a}+\vec{d}-\vec{e}_j), \\ &\qquad\qquad \Downarrow \\ &\alpha'\,\langle 1_j|\psi_0\rangle + \beta'\,\langle 1_j|\psi_1\rangle \in \mathcal{F}(\boldsymbol{\mathcal{N}}\setminus j, \vec{a}, \vec{d}-\vec{e}_j),\end{aligned} \tag{55}$$

where we used $\vec{e}_j$ to denote the vector that is one for the node μ such that qubit $j \in \mu$ and zero everywhere else. It is intuitive to understand that there is a generalization for this at each qubit that is lost. The resilience against any particle loss can be made larger by increasing the amount of ancillas. The privacy is guaranteed as, after loosing each qubit, we obtain a mixture of orthogonal states, which either have information about $\vec{a}$, as they belong to a family of private states, or they do not have information at all. To prove this consider:

Proposition 4.1. *Let* $|\psi\rangle \in \mathcal{F}(\boldsymbol{\mathcal{N}}, \vec{a}, \vec{d})$, $|\phi\rangle \in \mathcal{F}(\boldsymbol{\mathcal{N}}, \vec{a}, \vec{d}')$.

$$\vec{d} \neq \vec{d}' \implies \langle\psi|\phi\rangle = 0$$

Proof. The proof comes straightforward from realizing that distributed s-states are orthogonal if their generating strings s have different vectorial Hamming-weights. □

Proposition 4.2. *Let* $\Psi = \{|\psi_1\rangle, \ldots, |\psi_n\rangle\}$ *be a collection of states of a private family,* $|\psi_j\rangle \in \mathcal{F}(\boldsymbol{\mathcal{N}}, \vec{a}, \vec{d})\ \forall\ j = 1, \ldots, n$.

$$|\Psi\rangle = \sum_{j=1}^{n} \alpha_j\,|\psi_j\rangle \in \mathcal{F}(\boldsymbol{\mathcal{N}}, \vec{a}, \vec{d})\ \forall\ \alpha_j \in \mathbb{C} : \sum_{j=1}^{n} |\alpha_j|^2$$

Proof. The proof comes again straightforward as $|\Psi\rangle$ will only contain vectors belonging to $\mathcal{D}(\boldsymbol{\mathcal{N}}, \vec{d})$ and $\mathcal{D}(\boldsymbol{\mathcal{N}}, \vec{a} + \vec{d})$. □

Using this we are now able to prove the following theorem:

Theorem 4.1. *All the private states in the region of minimal plus ancilla amount of resources are able to either remain completely private under $\vec{e}$-qubit loss, if the amount of ancillas are at least $\vec{b} \succeq \vec{e}$, or provide no information at all.*

Proof. Any state belonging to the family of private states on $\mathcal{F}(\boldsymbol{\mathcal{N}}, \vec{a}, \vec{d})$, with associated vector of resources $\vec{n} = \vec{a} + \vec{b}$ already verifies privacy, by construction (Prop. 3.7). The evolution of these states under loss can be seen from Eqs. 54,55. Note that after the partial trace of each qubit we will have a mixture of states that belong to private families. We can group them according to the families they belong to, ensuring the states in the mixture are orthogonal and then using Prop. 4.1 and Eq. 37 to verify privacy. In the case they belong to the same family, diagonalizing them makes, by Prop. 4.2, new orthogonal states belonging to the same family. Nonetheless in this last case by analyzing Eq. 37 we also verify that this remains private. Applying the same procedure as in these equations to all qubits $j \in \vec{e}$, we get that the final eigenstates of the density matrix all belong to either private families, or are states with zero information at hand. □

4.7 Generalizing Results

When addressing the most general case, we use the private logical states introduced in Def. 3.7. For this, there is a condition to be able to use noise resiliency strategies already reproduced for single-parameter quantum metrology, and achieve the same outcome for multiparameter private metrology. The property is the following:

Condition 4.1. *We say a logical qubit basis $\{|0_L\rangle, |1_L\rangle\}$ is private against an error generated by a quantum channel $\mathcal{E}(\cdot)$ if:*

$$\forall \alpha, \beta \in \mathcal{C} : |\psi\rangle = \alpha |0_L\rangle + \beta |1_L\rangle, \mathcal{E}(|\psi\rangle\langle\psi|) = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|, \tag{56}$$

such that $\langle\psi_i|\psi_j\rangle = \delta_{ij}$ and $\exists \gamma : \langle\psi_i|\boldsymbol{G}_\mu|\psi_j\rangle = \gamma a_\mu$, for all i, j.

This allows us to say that, if a logical qubit basis is private against an error, then any state generated in that basis will also be private, under that same error. The consequence follows trivially from Eq. 37. This is already the case for the states in the minimal privacy zone under dephasing, depolarising and amplitude-damping noises and for minimal plus ancillas private states under particle loss.

5 Discussion of the Results

We have condensed the results of this work for the existence of private families of states with the corresponding assumptions and theorems in Table 1.

Throughout this paper we presented several families of states, which hold an important property for distributed sensing scenarios. Privacy comes as a natural consequence of choosing a state which makes available information about one single function of parameters. In all the results for pure states, the decomposition of the QFI in Eqs. 26 and 31 was crucial, and simplified the problem. Given its generality, one could potentially use this as means to efficiently calculate the QFI matrix, by following a similar procedure, and grouping states according to their vectorial Hamming weight.

Target	Hamiltonian	Resources	Private Family	Theorem
$\vec{a} \in \mathbb{R}^k$	Controlable (Fig. 2 d))	$\vec{n} = \vec{1}$	GHZ State	Thm. 3.4
$\vec{a} \in \mathbb{N}^k$	Separable (Fig. 2 a))	Zone (I)	None	Thms. 3.1, 3.3
		Zone (II)	GHZ State	Thms. 3.2, 3.4
		Zone (III)	Ancilla-Private States	Thm. 3.5
		Zone (IV)	Private Logical States	Thm. 3.6
$\vec{a} \in \mathcal{O}_-^2$	General (Fig. 2 b))	Depends on H	$\exists$ Private State	Thm. 3.7

Table 1: Main results regarding the existence of private states under the assumptions on the encoding dynamics, the target functions and the resources utilized.

The first no-go result is that, if one is not able to control the encoding dynamics, there is a minimum amount of resources such that one can estimate privately the target linear function, and this naturally depends on the Hamiltonian of the encoding dynamics. In particular, for separable Hamiltonians, with integer resources, one is only able to measure a linear function that is proportional to an integer combination of the parameters. The second result still for this class of Hamiltonians is, if we have exactly the amount of required resources, there is only one family of states that is able to estimate the target function privately, and this family is SLOCC equivalent to a GHZ state. Moreover, the GHZ state is the one for which the QFI is maximized, and therefore, the precision is also maximized. This result also affects the controllable encoding dynamics case, implying the privacy of a GHZ state with arbitrary number of qubit in each node. If one has n_μ on mode μ, and control over a linear parameter, t_μ, locally, then as long as one can make $n_\mu t_\mu = a_\mu$ for all μ, then one finds a private state.

Another important result is that, by adding extra qubits and superpositions of states that differ by local permutations, we can gain some redundancy, allowing us to create private states that maintain privacy and information even after qubit loss. This has important consequences for practical applications in near-term experiments.

Finally, we provide methods to analyze when multiples of the vector of resources are available. In this scenario, the scaling of the precision with the amount of resources is a pertinent question. In most cases, this is identical to dealing with the single parameter scenario by choosing logical qubits that are constituted by the basis of private states.

Moving to more general Hamiltonians, not necessarily separable, but still local in the sense that each node can only encode their own parameter, we found a structure on the space of available private functions and a way to generate the private states. However, in this scenario, it requires knowledge about the eigenstates of the Hamiltonian which is not a trivial problem, although there are some strategies to find them [63, 64]. Most importantly, this approach for general Hamiltonians provides an interesting insight to the structure of finding states for sensing. In particular it relates the maximum precision at which one can estimate a function employing a quantum sensing scheme and the privacy of such estimation, as they walk hand in hand. This was expected as the best local strategy is often to use locally entangled states, where the amount of information is the same, but scattered across each local parameter. When analyzing the best strategy for a given target function, privacy can also be perceived as an intuitive idea of concentrating all the information along a target function.

Overall, these results obtained clarify exactly which states one should build in order to perform secure and private from construction protocols for distributed quantum sensing. The continuity the privacy measure with respect to the QFI information, allows one to infer and create protocols that provide bounds on the QFI to establish bounds on the privacy

of a state. These bounds in the privacy can then be converted into security concerns by an appropriate protocol, as we have discussed, that uses state certification rounds intercalated with sensing rounds.

This work opens up a different way to look at sensing protocols, relating resources and hamiltonian dynamics to information directly. While the framework has been consistently that of quantum sensing, where measurements are repeated and from them estimators are created, one could potentially apply our results to distributed quantum computation. In particular, we dealt with only linear functions, which seems to be a consequence of the Hamiltonian dynamics not being able to encode arbitrary functions of parameters. A possible direction of future work could be coming up with protocols to access non-linear functions.

Another possible direction would be to find all of the private states when multiples of the vector of resources are available. Since technically from the definition of a Private-Ancilla state, these are not limited to $\vec{n} \preceq 2\vec{a}$, it is possible that finding all states involves constructing a hierarchy of private states by the logical encoding formalism taking the logical qubits inside each of the $(m\vec{a})$-Private-Ancilla states, $m = 1, 2, \ldots$, and verify possible repetitions of families by playing with different encodings.

Finally, the structure of the private orthotope, and the fact that it is an orthotope, might hint at some more fundamental results. It would be interesting to understand exactly are the implications of this, outside of the privacy in the sensing scenario, and into an information perspective by using the intuition of concentration of information.

Acknowledgements

The authors acknowledge the support from the EU Quantum Flagship project QIA (101102140) and France 2030 under the French National Research Agency projects HQI ANR-22-PNCQ-0002 and the PEPR integrated project EPiQ ANR-22-PETQ-0007. L.B. and Y.O. thank the support from Fundação para a Ciência e a Tecnologia (FCT, Portugal), namely through project UIDB/04540/2020. L.B. acknowledges the support of FCT through scholarship BD/05268/2021.

References

[1] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum metrology. *Physical Review Letters*, 96(1):13–16, 2006. ISSN 10797114. DOI: 10.1103/PhysRevLett.96.010401.

[2] Jasminder S. Sidhu and Pieter Kok. A Geometric Perspective on Quantum Parameter Estimation. *AVS Quantum Science*, 2(1):014701, July 2019. ISSN 2639-0213. DOI: 10.1116/1.5119961.

[3] C. L. Degen, F. Reinhard, and P. Cappellaro. Quantum sensing. *Reviews of Modern Physics*, 89(3):035002, July 2017. DOI: 10.1103/RevModPhys.89.035002.

[4] Zhibo Hou, Yan Jin, Hongzhen Chen, Jun-Feng Tang, Chang-Jiang Huang, Haidong Yuan, Guo-Yong Xiang, Chuan-Feng Li, and Guang-Can Guo. "Super-Heisenberg" and Heisenberg Scalings Achieved Simultaneously in the Estimation of a Rotating Field. *Physical Review Letters*, 126(7):70503, 2021. ISSN 1079-7114. DOI: 10.1103/PhysRevLett.126.070503.

[5] Li-Zheng Liu, Yu-Zhe Zhang, Zheng-Da Li, Rui Zhang, Xu-Fei Yin, Yue-Yang Fei, Li Li, Nai-Le Liu, Feihu Xu, Yu-Ao Chen, and Jian-Wei Pan. Distributed quantum

phase estimation with entangled photons. *Nature Photonics*, 15(2):137–142, February 2021. ISSN 1749-4885, 1749-4893. DOI: 10.1038/s41566-020-00718-2.

[6] Marco Barbieri. Optical Quantum Metrology. *PRX Quantum*, 3(1):010202, January 2022. ISSN 2691-3399. DOI: 10.1103/PRXQuantum.3.010202.

[7] Changhao Li, Mo Chen, and Paola Cappellaro. A geometric perspective: Experimental evaluation of the quantum Cramer-Rao bound, April 2022, arXiv:2204.13777. DOI: 10.48550/arXiv.2204.13777.

[8] Matteo G.A. Paris. Quantum estimation for quantum technology. *International Journal of Quantum Information*, 7(SUPPL.):125–137, 2009. ISSN 02197499. DOI: 10.1142/S0219749909004839.

[9] Stephanie Wehner, David Elkouss, and Ronald Hanson. Quantum internet: A vision for the road ahead. *Science*, 362(6412):eaam9288, October 2018. ISSN 10959203. DOI: 10.1126/science.aam9288.

[10] T. J. Proctor, P. A. Knott, and J. A. Dunningham. Networked quantum sensing, February 2017, arXiv:1702.04271. DOI: 10.48550/arXiv.1702.04271.

[11] Raja Yehia, Simon Neves, Eleni Diamanti, and Iordanis Kerenidis. Quantum City: Simulation of a practical near-term metropolitan quantum network, November 2022, arXiv:2211.01190. DOI: 10.48550/arXiv.2211.01190.

[12] Pavel Sekatski, Sabine Wölk, and Wolfgang Dür. Optimal distributed sensing in noisy environments. *Physical Review Research*, 2(2):1–8, May 2019. DOI: 10.1103/PhysRevResearch.2.023052.

[13] P. A. Knott, T. J. Proctor, A. J. Hayes, J. F. Ralph, P. Kok, and J. A. Dunningham. Local versus global strategies in multiparameter estimation. *Physical Review A*, 94 (6):062312, December 2016. DOI: 10.1103/PhysRevA.94.062312.

[14] Zachary Eldredge, Michael Foss-Feig, Jonathan A. Gross, Steven L. Rolston, and Alexey V. Gorshkov. Optimal and secure measurement protocols for quantum sensor networks. *Physical Review A*, 97(4):042337, April 2018. ISSN 2469-9926. DOI: 10.1103/PhysRevA.97.042337.

[15] Timothy J. Proctor, Paul A. Knott, and Jacob A. Dunningham. Multiparameter Estimation in Networked Quantum Sensors. *Physical Review Letters*, 120(8):1–11, 2018. ISSN 10797114. DOI: 10.1103/PhysRevLett.120.080501.

[16] Kevin Qian, Zachary Eldredge, Wenchao Ge, Guido Pagano, Christopher Monroe, J. V. Porto, and Alexey V. Gorshkov. Heisenberg-scaling measurement protocol for analytic functions with quantum sensor networks. *Physical Review A*, 100(4):042304, October 2019. ISSN 2469-9926. DOI: 10.1103/PhysRevA.100.042304.

[17] Zheshen Zhang and Quntao Zhuang. Distributed Quantum Sensing, October 2020, arXiv:2010.14744. DOI: 10.48550/arXiv.2010.14744.

[18] Timothy Qian, Jacob Bringewatt, Igor Boettcher, Przemyslaw Bienias, and Alexey V. Gorshkov. Optimal measurement of field properties with quantum sensor networks. *Physical Review A*, 103(3):L030601, March 2021. ISSN 2469-9926. DOI: 10.1103/PhysRevA.103.L030601.

[19] Huan Cao, Chao Zhang, Yun-Feng Huang, Bi-Heng Liu, Chuan-Feng Li, Philip Walther, and Guang-Can Guo. Experimental beating the standard quantum limit under non-markovian dephasing environment, August 2022, arXiv:2208.02543. DOI: 10.48550/arXiv.2208.02543.

[20] Peter Kómár, Eric M. Kessler, Michael Bishof, Liang Jiang, Anders S. Sørensen, Jun Ye, and Mikhail D. Lukin. A quantum network of clocks. *Nature Physics*, 10(8): 582–587, October 2013. ISSN 1745-2473. DOI: 10.1038/nphys3000.

[21] B. C. Nichol, R. Srinivas, D. P. Nadlinger, P. Drmota, D. Main, G. Araneda, C. J. Ballance, and D. M. Lucas. An elementary quantum network of entangled optical atomic clocks. *Nature*, 609(7928):689–694, September 2022. ISSN 1476-4687. DOI: 10.1038/s41586-022-05088-z.

[22] Emil T. Khabiboulline, Johannes Borregaard, Kristiaan De Greve, and Mikhail D. Lukin. Optical Interferometry with Quantum Networks. *Physical Review Letters*, 123 (7):070504, September 2018. ISSN 0031-9007. DOI: 10.1103/PhysRevLett.123.070504.

[23] T. Lévèque, C. Fallet, M. Mandea, R. Biancale, J. M. Lemoine, S. Tardivel, S. Delavault, A. Piquereau, S. Bourgogne, F. Pereira Dos Santos, B. Battelier, and Ph Bouyer. Gravity field mapping using laser-coupled quantum accelerometers in space. *Journal of Geodesy*, 95(1):1–19, 2021. ISSN 14321394. DOI: 10.1007/s00190-020-01462-9.

[24] Lorcán O. Conlon, Thibault Michel, Giovanni Guccione, Kirk McKenzie, Syed M. Assad, and Ping Koy Lam. Enhancing the precision limits of interferometric satellite geodesy missions. *npj Microgravity*, 8(1):1–10, June 2022. ISSN 2373-8065. DOI: 10.1038/s41526-022-00204-9.

[25] Anthony J. Brady, Xin Chen, Kewen Xiao, Yi Xia, Zhen Liu, Roni Harnik, Dalziel J. Wilson, Zheshen Zhang, and Quntao Zhuang. Entanglement-enhanced optomechanical sensor array for dark matter searches. *Commun Phys*, 6(237), 2023. https://doi.org/10.1038/s42005-023-01357-z.

[26] Ivan Alonso et al. Cold Atoms in Space: Community Workshop Summary and Proposed Road-Map. *EPJ Quantum Technology*, 9(1):30, December 2022. ISSN 2662-4400, 2196-0763. https://doi.org/10.1140/epjqt/s40507-022-00147-w.

[27] B Fang, I Dutta, P Gillot, D Savoie, J Lautier, B Cheng, C L Garrido Alzar, R Geiger, S Merlet, F Pereira Dos Santos, and A Landragin. Metrology with Atom Interferometry: Inertial Sensors from Laboratory to Field Applications. *Journal of Physics: Conference Series*, 723:012049, June 2016. ISSN 1742-6588, 1742-6596. DOI: 10.1088/1742-6596/723/1/012049.

[28] Graham P. Greve, Chengyi Luo, Baochen Wu, and James K. Thompson. Entanglement-enhanced matter-wave interferometry in a high-finesse cavity. *Nature*, 610(7932):472–477, October 2022. ISSN 1476-4687. DOI: 10.1038/s41586-022-05197-9.

[29] Bálint Koczor, Suguru Endo, Tyson Jones, Yuichiro Matsuzaki, and Simon C. Benjamin. Variational-state quantum metrology. *New Journal of Physics*, 22(8):1–14, August 2020. ISSN 13672630. DOI: 10.1088/1367-2630/ab965e.

[30] Johannes Jakob Meyer, Johannes Borregaard, and Jens Eisert. A variational toolbox for quantum multi-parameter estimation. *npj Quantum Information*, 7(1):89, December 2021. ISSN 20566387. DOI: 10.1038/s41534-021-00425-y.

[31] Raphael Kaubruegger, Athreya Shankar, Denis V. Vasilyev, and Peter Zoller. Optimal and Variational Multi-Parameter Quantum Metrology and Vector Field Sensing. *PRX Quantum*, 4(020333), June 2023. DOI: 10.1103/PRXQuantum.4.020333.

[32] Shuhong Hao, Haowei Shi, Christos N. Gagatsos, Mayank Mishra, Boulat Bash, Ivan Djordjevic, Saikat Guha, Quntao Zhuang, and Zheshen Zhang. Demonstration of Entanglement-Enhanced Covert Sensing. *Physical Review Letters*, 129(1):010501, June 2022. DOI: 10.1103/PhysRevLett.129.010501.

[33] Hiroto Kasai, Yuki Takeuchi, Hideaki Hakoshima, Yuichiro Matsuzaki, and Yasuhiro Tokura. Anonymous Quantum Sensing. *Journal of the Physical Society of Japan*, 91 (7):074005, July 2022. ISSN 0031-9015. DOI: 10.7566/JPSJ.91.074005.

[34] Nathan Shettell, William J. Munro, Damian Markham, and Kae Nemoto. Practical

limits of error correction for quantum metrology. *New Journal of Physics*, 23(4): 043038, April 2021. ISSN 1367-2630. DOI: 10.1088/1367-2630/abf533.

[35] Kaoru Yamamoto, Suguru Endo, Hideaki Hakoshima, Yuichiro Matsuzaki, and Yuuki Tokunaga. Error-Mitigated Quantum Metrology via Virtual Purification. *Physical Review Letters*, 129(25):250503, December 2022. DOI: 10.1103/PhysRevLett.129.250503.

[36] Jing Liu and Haidong Yuan. Control-enhanced multiparameter quantum estimation. *Physical Review A*, 96(4), 2017. ISSN 24699934. DOI: 10.1103/PhysRevA.96.042114.

[37] Jesús Rubio and Jacob Dunningham. Bayesian multiparameter quantum metrology with limited data. *Physical Review A*, 101(3), 2020. ISSN 24699934. DOI: 10.1103/PhysRevA.101.032114.

[38] Jesús Rubio, Paul A. Knott, Timothy J. Proctor, and Jacob A. Dunningham. Quantum sensing networks for the estimation of linear functions. *Journal of Physics A: Mathematical and Theoretical*, 53(34):344001, March 2020. ISSN 1751-8113. DOI: 10.1088/1751-8121/ab9d46.

[39] Jacob Bringewatt, Igor Boettcher, Pradeep Niroula, Przemyslaw Bienias, and Alexey V. Gorshkov. Protocols for estimating multiple functions with quantum sensor networks: Geometry and performance. *Physical Review Research*, 3(3):033011, July 2021. DOI: 10.1103/PhysRevResearch.3.033011.

[40] Nathan Shettell, Elham Kashefi, and Damian Markham. Cryptographic approach to quantum metrology. *Physical Review A*, 105(1):L010401, January 2022. DOI: 10.1103/PhysRevA.105.L010401.

[41] Sean William Moore and Jacob Andrew Dunningham. Secure Quantum Remote Sensing Without Entanglement, February 2023, arXiv:2302.03617. DOI: 10.48550/arXiv.2302.03617.

[42] Nathan Shettell, Majid Hassani, and Damian Markham. Private network parameter estimation with quantum sensors, July 2022, arXiv:2207.14450. DOI: 10.48550/arXiv.2207.14450.

[43] Nathan Shettell and Damian Markham. Graph States as a Resource for Quantum Metrology. *Physical Review Letters*, 124(11):110502, March 2020. ISSN 0031-9007. DOI: 10.1103/PhysRevLett.124.110502.

[44] Jing Liu, Haidong Yuan, Xiao-Ming Lu, and Xiaoguang Wang. Quantum Fisher information matrix and multiparameter estimation. *Journal of Physics A: Mathematical and Theoretical*, 53(2):023001, December 2019. ISSN 1751-8121. DOI: 10.1088/1751-8121/ab5d4d.

[45] Aaron Z. Goldberg, Luis L. Sánchez-Soto, and Hugo Ferretti. Intrinsic Sensitivity Limits for Multiparameter Quantum Metrology. *Physical Review Letters*, 127(11): 110501, September 2021. DOI: 10.1103/PhysRevLett.127.110501.

[46] Jarrod T. Reilly, John Drew Wilson, Simon B. Jäger, Christopher Wilson, and Murray J. Holland. Optimal Generators for Quantum Sensing. *Physical Review Letters*, 131(150802), October 2023. 2010. DOI: 10.1103/PhysRevLett.131.150802.

[47] Marcin Zwierz, Carlos A. Pérez-Delgado, and Pieter Kok. General optimality of the Heisenberg limit for quantum metrology. *Physical Review Letters*, 105(18):1–4, 2010. ISSN 00319007. DOI: 10.1103/PhysRevLett.105.180402.

[48] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information*, volume 52. 2011. ISBN 978-1-107-00217-3. DOI: 10.1080/00107514.2011.587535.

[49] Shettell, Nathan and Markham, Damian Quantum Metrology with Delegated Tasks. *Physical Review A*, 106(5):052427, 2022. DOI: 10.1103/PhysRevA.106.052427.

[50] Sammy Ragy, Marcin Jarzyna, and Rafał Demkowicz-Dobrzański. Compatibility in

multiparameter quantum metrology. *Physical Review A*, 94(5):052108, November 2016. ISSN 2469-9926, 2469-9934. DOI: 10.1103/PhysRevA.94.052108.

[51] Anupama Unnikrishnan and Damian Markham. Verification of graph states in an untrusted network. *Physical Review A*, 105(5):052420, May 2022. DOI: 10.1103/PhysRevA.105.052420.

[52] M. Hein, J. Eisert, and H. J. Briegel. Multiparty entanglement in graph states. *Physical Review A - Atomic, Molecular, and Optical Physics*, 69(6):1–22, 2004. ISSN 10502947. DOI: 10.1103/PhysRevA.69.062311.

[53] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, and H. J. Briegel. Entanglement in Graph States and its Applications. *Proceedings of the International School of Physics "Enrico Fermi"*, 162:115–218, February 2006. ISSN 0074784X. DOI: 10.3254/978-1-61499-018-5-115.

[54] Scott Aaronson and Daniel Gottesman. Improved simulation of stabilizer circuits. *Physical Review A - Atomic, Molecular, and Optical Physics*, 70(5 A):1–14, 2004. ISSN 10502947. DOI: 10.1103/PhysRevA.70.052328.

[55] Nathan Shettell. *Quantum Information Techniques for Quantum Metrology*. PhD thesis, 2022. DOI: 10.48550/arXiv.2201.01523.

[56] Hong Tao and Xiaoqing Tan Quantum multiparameter estimation with graph states, June 2023, arXiv:2306.02518. DOI: 10.48550/arXiv.2306.02518.

[57] Rafał Demkowicz-Dobrzański, Jan Czajkowski, and Pavel Sekatski. Adaptive Quantum Metrology under General Markovian Noise. *Physical Review X*, 7(4):041009, October 2017. ISSN 2160-3308. DOI: 10.1103/PhysRevX.7.041009.

[58] Yingkai Ouyang, Nathan Shettell, and Damian Markham. Robust quantum metrology with explicit symmetric states. *IEEE Transactions on Information Theory*, 68(3): 1809–1821, March 2022. ISSN 0018-9448, 1557-9654. DOI: 10.1109/TIT.2021.3132634.

[59] Masahito Hayashi, Zi-Wen Liu, and Haidong Yuan. Global Heisenberg scaling in noisy and practical phase estimation. *Quantum Science and Technology*, 7(2):025030, April 2022. ISSN 2058-9565. DOI: 10.1088/2058-9565/ac5d7e.

[60] A. T. Rezakhani, M. Hassani, and S. Alipour. Continuity of the quantum Fisher information. *Physical Review A*, 100(3):32317, 2019. ISSN 24699934. DOI: 10.1103/PhysRevA.100.032317.

[61] Luís Bugalho, Bruno C. Coutinho, Francisco A. Monteiro, and Yasser Omar. Distributing Multipartite Entanglement over Noisy Quantum Networks. *Quantum*, 7: 920, February 2023. DOI: 10.22331/q-2023-02-09-920.

[62] Reinhard F. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Physical Review A*, 40(8):4277–4281, 1989. ISSN 10502947. DOI: 10.1103/PhysRevA.40.4277.

[63] Raffaele Santagati, Jianwei Wang, Antonio A. Gentile, Stefano Paesani, Nathan Wiebe, Jarrod R. McClean, Sam Morley-Short, Peter J. Shadbolt, Damien Bonneau, Joshua W. Silverstone, David P. Tew, Xiaoqi Zhou, Jeremy L. O'Brien, and Mark G. Thompson. Witnessing eigenstates for quantum simulation of Hamiltonian spectra. *Science Advances*, 4(1):eaap9646, January 2018. DOI: 10.1126/sciadv.aap9646.

[64] Richard Meister and Simon C. Benjamin. Resource-frugal Hamiltonian eigenstate preparation via repeated quantum phase estimation measurements, December 2022, arXiv:2212.00846. DOI: 10.48550/arXiv.2212.00846.

A Unitary Equivalence of Encoding Dynamics

In this appendix we go over the proofs of the interplay between the dynamics and the initial state. Starting by restating the first theorem:

Lemma 2.1. *Consider two different generators for single qubit unitary operators G and G', and a unitary operator W.*

$$\forall G, G'; \exists W : W^\dagger G W = G'$$

Proof. Since G and G' are generators for single qubit unitary operators, then they can be decomposed into a linear combination of Pauli operators. Let them be $G = \vec{a} \cdot \vec{\sigma}$ and $G' = \vec{b} \cdot \vec{\sigma}$, such that $|\vec{a}| = |\vec{b}| = 1$. Using the expression for the adjoint action on the Pauli vector

$$R_{\vec{n}}(-\alpha)\ \vec{\sigma}\ R_{\vec{n}}(\alpha) = \vec{\sigma}\cos(\alpha) + \vec{n} \times \vec{\sigma}\sin(\alpha) + \vec{n}\ \vec{n} \cdot \vec{\sigma}(1 - \cos(\alpha)) \tag{57}$$

Taking the inner product with $\vec{a}$ we get that:

$$\begin{aligned} R_{\vec{n}}(-\alpha)\ \vec{a} \cdot \vec{\sigma}\ R_{\vec{n}}(\alpha) &= \vec{a} \cdot \vec{\sigma}\cos(\alpha) + \vec{a} \cdot (\vec{n} \times \vec{\sigma})\sin(\alpha) + \vec{a} \cdot \vec{n}\ \vec{n} \cdot \vec{\sigma}(1 - \cos(\alpha)) \\ &= [\vec{a}\cos(\alpha) + \vec{a} \times \vec{n}\sin(\alpha) + \vec{n}\ \vec{a} \cdot \vec{n}(1 - \cos(\alpha))] \cdot \vec{\sigma} \\ &= \left[\mathbb{1}\cos(\alpha) + \vec{n}\vec{n}^T(1 - \cos(\alpha)) + [\vec{n}]_\times \sin(\alpha)\right] \vec{a} \cdot \vec{\sigma} \\ &= (R_{\vec{n}}^{xyz}(\alpha)\vec{a}) \cdot \vec{\sigma} \\ &= \vec{b} \cdot \vec{\sigma}, \end{aligned}$$

where $R_{\vec{n}}^{xyz}(\alpha)$ is the rotation in $\mathbb{R}^3$ around the axis $\vec{n}$, by an angle of α. This in turn means that we can always find values for $\vec{n}$ and α such that one can transform the vector $\vec{a}$ into vector $\vec{b}$. Setting $W = R_{\vec{n}}(\alpha)$ we can always find a unitary transformation that transforms one generator into another. □

Which consequently leads to:

Corollary 2.1 (Interplay Dynamics ↔ Initial State)**.** *Consider two different unitary encodings, in terms of two different generators $U_\theta = e^{-i\theta G}$ and $U'_\theta = e^{-i\theta G'}$, and a unitary operator W.*

$$\forall U_\theta, U'_\theta; \exists W : W^\dagger U_\theta W = U'_\theta$$

Proof. Follows trivially from previous theorem:

$$\begin{aligned} W^\dagger U_\theta W &= W^\dagger e^{-i\theta G} W \\ &= W^\dagger \left[\mathbb{1} + \frac{-i\theta}{1!}G + \frac{(-i\theta)^2}{2!}G^2 + ...\right] W \\ &= W^\dagger W + \frac{-i\theta}{1!}W^\dagger G W + \frac{(-i\theta)^2}{2!}W^\dagger G^2 W + ... \\ &= \mathbb{1} + \frac{-i\theta}{1!}W^\dagger G W + \frac{(-i\theta)^2}{2!}W^\dagger G W W^\dagger G W + ... \\ &= \mathbb{1} + \frac{-i\theta}{1!}G' + \frac{(-i\theta)^2}{2!}G'^2 + ... \\ &= e^{-i\theta G'}. \end{aligned}$$

□

B Privacy Measure

In this appendix we look at the measure of privacy introduced in Def. 2.3, and prove the properties it should follow, introduced in the main text. Looking at the second and third properties, they should come by construction, as we verify below. For the last two, it is not obvious, but we still get them:

2. From the fact that $\mathcal{Q}$ is a positive semi-definite matrix, we get that $\mathcal{P}(\mathcal{Q}, \vec{a}) \leq 1$. The minimum value follows from:

$$\begin{aligned} \frac{\vec{a}^T \mathcal{Q} \vec{a}}{\operatorname{Tr} \mathcal{Q}} &= \frac{\vec{a}^T \sum_i \beta_i \vec{b}_i \vec{b}_i^T \vec{a}}{\operatorname{Tr} \mathcal{Q}} \\ &= \frac{\sum_i \beta_i (\vec{a} \cdot \vec{b}_i)^2}{\operatorname{Tr}\left[\sum_i \beta_i \vec{b}_i \vec{b}_i^T\right]} \\ &= \frac{\sum_i \beta_i (\vec{a} \cdot \vec{b}_i)^2}{\sum_i \beta_i} \\ &\leq 1, \end{aligned} \tag{58}$$

   as $\vec{a} \cdot \vec{b}_i \leq 1$ always, choosing normalized vectors $\vec{b}_i$.

3. The fact that only a QFI of the type $\mathcal{Q} = \alpha \vec{a} \vec{a}^T$ saturates the bounds comes trivially from before, as $\vec{a} \cdot \vec{b}_i = 1$ iff $\vec{b}_i = \vec{a}$. Moreover, even if the QFI does not come in a diagonal form, we can still show that:

$$\begin{aligned} \frac{\vec{a}^T \mathcal{Q} \vec{a}}{\operatorname{Tr} \mathcal{Q}} &= \frac{\vec{a}^T \sum_{ij} \beta_{ij} \vec{b}_i \vec{b}_j^T \vec{a}}{\operatorname{Tr} \mathcal{Q}} \\ &= \frac{\vec{a}^T \sum_i \tilde{\beta}_i \vec{\tilde{b}}_i \vec{\tilde{b}}_i^T \vec{a}}{\operatorname{Tr} \mathcal{Q}} \\ &= \frac{\sum_i \tilde{\beta}_i (\vec{a} \cdot \vec{\tilde{b}}_i)^2}{\sum_i \tilde{\beta}_i} \\ &\leq 1, \end{aligned} \tag{59}$$

   as the matrix of the QFI $\mathcal{Q}$ is always real and symmetric, so there is always a diagonalization for it. Moreover, since it is positive semi-definite matrix all $\tilde{\beta}_i$ are positive. The only way the bound is saturated is if $\exists i : \vec{\tilde{b}}_i = \vec{a}$ and $\tilde{\beta}_j = 0 \forall j \neq i$.

4. $$\begin{aligned} \mathcal{P}(B\mathcal{Q}B^T, B\vec{a}) &= \frac{\operatorname{Tr} B\mathcal{Q}B^T - \vec{a}^T B^T B \mathcal{Q} B^T B \vec{a}}{\operatorname{Tr} B\mathcal{Q}B^T} \\ &= \frac{\operatorname{Tr} \mathcal{Q}B^T B - \vec{a}^T \mathcal{Q} \vec{a}}{\operatorname{Tr} \mathcal{Q}B^T B} \\ &= \frac{\operatorname{Tr} \mathcal{Q} - \vec{a}^T \mathcal{Q} \vec{a}}{\operatorname{Tr} \mathcal{Q}} \\ &= \mathcal{P}(\mathcal{Q}, \vec{a}), \end{aligned} \tag{60}$$

   where we made the assumption that B is a orthonormal change of basis matrix, *i.e.* $BB^T = \mathbb{1}$. In case it is not, the two measures are not equivalent, but they still present a valid skewed measure.

5.

$$\begin{aligned}
\mathcal{P}(\mathcal{Q}+\epsilon A,\vec{a})-\mathcal{P}(\mathcal{Q},\vec{a}) &= \frac{\operatorname{Tr}\left[\mathcal{Q}+\epsilon A\right]-\vec{a}^T(\mathcal{Q}+\epsilon A)\vec{a}}{\operatorname{Tr}\left[\mathcal{Q}+\epsilon A\right]}-\frac{\operatorname{Tr}\mathcal{Q}-\vec{a}^T\mathcal{Q}\vec{a}}{\operatorname{Tr}\mathcal{Q}} \\
&= 1-\frac{\vec{a}(\mathcal{Q}+\epsilon A)\vec{a}^T}{\operatorname{Tr}\mathcal{Q}+\epsilon\operatorname{Tr}A}-\left(1-\frac{\vec{a}\mathcal{Q}\vec{a}^T}{\operatorname{Tr}\mathcal{Q}}\right) \\
&= \frac{\vec{a}\mathcal{Q}\vec{a}^T}{\operatorname{Tr}\mathcal{Q}}-\frac{\vec{a}\mathcal{Q}\vec{a}^T}{\operatorname{Tr}\mathcal{Q}+\epsilon\operatorname{Tr}A}-\epsilon\frac{\vec{a}A\vec{a}^T}{\operatorname{Tr}\mathcal{Q}+\epsilon\operatorname{Tr}A} \\
|\mathcal{P}(\mathcal{Q}+\epsilon A,\vec{a})-\mathcal{P}(\mathcal{Q},\vec{a})| &\leq \left|\frac{\vec{a}\mathcal{Q}\vec{a}^T}{\operatorname{Tr}\mathcal{Q}+\epsilon\operatorname{Tr}A}+\epsilon\frac{\vec{a}A\vec{a}^T}{\operatorname{Tr}\mathcal{Q}+\epsilon\operatorname{Tr}A}-\frac{\vec{a}\mathcal{Q}\vec{a}^T}{\operatorname{Tr}\mathcal{Q}}\right| \\
&\leq \left|\frac{\vec{a}\mathcal{Q}\vec{a}^T}{\operatorname{Tr}\mathcal{Q}}+\epsilon\frac{\vec{a}A\vec{a}^T}{\operatorname{Tr}\mathcal{Q}}-\frac{\vec{a}\mathcal{Q}\vec{a}^T}{\operatorname{Tr}\mathcal{Q}}\right| \\
&= \left|\epsilon\frac{\vec{a}A\vec{a}^T}{\operatorname{Tr}\mathcal{Q}}\right|\equiv\delta,
\end{aligned} \tag{61}$$

providing the continuity of the privacy upon change of the initial state.

Using this measure of private one can try and understand what the different values of $\mathcal{P}$ mean. The complete private case $\mathcal{P}=1$ can be verified to naturally satisfy all conditions for the privacy. If the QFI matrix is of the form $\mathcal{Q}=\alpha\vec{a}\vec{a}^T$ then is only possible to find an estimator for the function $f(\boldsymbol{\theta})=\vec{a}\cdot\vec{\boldsymbol{\theta}}$. This also means that whatever estimators for other functions would be ill-defined and not accessible (infinite variance). Consequently all parties can not estimate but the target function, and the dishonest parties having access to all the values in the dishonest subset, could at most gather information about the honest parties function $f(\boldsymbol{\theta}_H)$ but not their local values. Here and henceforth, taking a vector of distributed parameters $\vec{a}$, we will denote $\vec{a}_H$ has the subset of the same vector belonging to the honest parties.

For the case of $\mathcal{P}=\epsilon$ let us provide two examples to understand how ϵ would affect the information that might be leaked in the case of dishonest parties:

Example B.1. *Suppose the QFI matrix is given by:*

$$\mathcal{Q}=\epsilon\vec{a}\vec{a}^T+(1-\epsilon)\vec{b}\vec{b}^T,$$

such that $\vec{a}_H\cdot\vec{b}_H=0$, $\vec{a}\cdot\vec{b}=0$, denoting by $\vec{x}_H$ the vector restricted to the honest parties. First verify that $\mathcal{P}=\epsilon$ for the estimation of the function $f(\boldsymbol{\theta})=\vec{a}\cdot\vec{\boldsymbol{\theta}}$. Then, since the dishonest parties can share their own values and therefore have access to all $\theta_\mu\in D$, they also have access to $\vec{b}_H\cdot\vec{\boldsymbol{\theta}}$ which is a different from $f(\boldsymbol{\theta}_H)$, which is the private function. This is not private, since it violates the third condition of privacy. If $\epsilon=0$, then their information about this function is the maximum possible for this estimation ($\operatorname{Tr}\mathcal{Q}$).

Example B.2. *Suppose we have k parties and $d\leq k/2$ dishonest parties among them. Le the QFI matrix be given by:*

$$\mathcal{Q}=\epsilon\vec{a}\vec{a}^T+\frac{1-\epsilon}{d}\sum_{j=1}^{d}\vec{b}_j\vec{b}_j^T,$$

Such that $\vec{a}\cdot\vec{b}_j=0$ for all vectors $\vec{b}_j$. In particular, one can choose these vectors $\vec{b}_j$ such that $\vec{b}_{j_H}$, which is the correspondent to slicing the vectors $\vec{b}_j$ for the indices correspondent to

honest parties, form a d-dimensional orthogonal subspace. Again, we first verify that $\mathcal{P} = \epsilon$ *as every* $\vec{b}_j$ *is orthogonal to* $\vec{a}$*. Second, we verify that the set of information available by considering every dishonest party knows the dishonest subspace, is given by an orthogonal basis of* d *vectors in the honest subspace. Namely they have information about all* $\vec{b}_{j_H} \cdot \vec{\boldsymbol{\theta}}$ *after using the dishonest information. In particular, if* $d = k/2$*, then they have* d *linearly independent vectors to estimate the honest subspace with* $k - d = d$ *functions. This means they also have access to each individual parameter of the honest parties. Again, if* $\epsilon \to 0$ *then they are more efficient, in the sense the variance at which they can do this the same amount of resources is smaller.*

Note however that in both of these cases, for the parties to implement a non-private strategy and acquire information about the honest parties, they would have to distribute a non-private state. If one utilizes a state certification protocol in conjunction with this [42], then one can guarantee privacy and security.

C Integer Vectors Properties

Proposition 3.3. $\forall\ \vec{a}, \vec{b} \in \mathbb{Z}^k$ *such that* $gcd(\vec{a}) = 1$ *then, if* $\vec{b} = \alpha\vec{a}$ *implies that* $\alpha \in \mathbb{Z}$*.*

Proof. If $\alpha \in \mathbb{Z}$, then $\vec{a} \in \mathbb{Z}^k \implies \vec{b} \in \mathbb{Z}^k$. To prove it is the only option choose a b_i such that $b_i = \alpha a_i$, where $\alpha \notin \mathbb{Z} = c/d$. For b_j to be integer for every other j, then $gcd(\vec{a}, d) > 1$, as in, every a_i. However, gcd is associative, meaning $gcd(\vec{a}, d) = gcd(gcd(\vec{a}), d) = 1$. This means α has to be integer. □

Proposition 3.4. *Let* $\vec{m}$ *be a integer vector in* $\mathbb{Z}_+^k$ *such that* $gcd(\vec{m}) = 1$*. Then:*

$$\nexists\ \vec{a} \neq \vec{b} \in \mathbb{Z}_+^k, \vec{a}, \vec{b} \prec \vec{m} : (\vec{m} - 2\vec{a}) \pm (\vec{m} - 2\vec{b}) = \alpha\vec{m} \quad , \quad \alpha \neq 0.$$

Proof. Since $\vec{a}, \vec{b} \prec \vec{m}, \vec{0} \prec \vec{a} + \vec{b} \prec 2\vec{m}, -\vec{m} \prec \vec{a} - \vec{b} \prec \vec{m}$. $gcd(\vec{m}) = 1 \implies$ if $\alpha\vec{m} \propto \vec{m}$ then $\alpha \in \mathbb{Z}$.

$$\Leftrightarrow \begin{cases} 2\left[\vec{m} - \left(\vec{a} + \vec{b}\right)\right] \propto \vec{m} \\ 2\left(\vec{a} - \vec{b}\right) \propto \vec{m} \end{cases} \Leftrightarrow \begin{cases} \left[\vec{m} - \left(\vec{a} + \vec{b}\right)\right] \propto \vec{m} \\ \left(\vec{a} - \vec{b}\right) \propto \vec{m} \end{cases} \text{ but } \begin{cases} -\vec{m} \prec \vec{m} - \left(\vec{a} + \vec{b}\right) \prec \vec{m} \\ -\vec{m} \prec \vec{a} - \vec{b} \prec \vec{m} \end{cases} . \tag{62}$$

□

Proposition 3.5. *Let* $\vec{m}$ *be a target vector in* $\mathbb{Z}_+^k$ *such that* $gcd(\vec{m}) = 1$*. Let* $\vec{n}$ *be a resource vector in the same space, such that* $\vec{n} \not\succeq \vec{m}$*. Then:*

$$\nexists\ \vec{a} \neq \vec{b} \in \mathbb{Z}_+^k, \vec{a}, \vec{b} \prec \vec{n} : (\vec{n} - 2\vec{a}) \pm (\vec{n} - 2\vec{b}) = \alpha\vec{m} \quad , \quad \alpha \neq 0.$$

Proof. The proof follows similarly. Since $\vec{a}, \vec{b} \prec \vec{n}, \vec{0} \prec \vec{a} + \vec{b} \prec 2\vec{n}, -\vec{n} \prec \vec{a} - \vec{b} \prec \vec{n}$. $gcd(\vec{m}) = 1 \implies$ if $\alpha\vec{m} \propto \vec{m}$ then $\alpha \in \mathbb{Z}$.

$$\Leftrightarrow \begin{cases} 2\left[\vec{n} - \left(\vec{a} + \vec{b}\right)\right] \propto \vec{m} \\ 2\left(\vec{a} - \vec{b}\right) \propto \vec{m} \end{cases} \Leftrightarrow \begin{cases} \left[\vec{n} - \left(\vec{a} + \vec{b}\right)\right] \propto \vec{m} \\ \left(\vec{a} - \vec{b}\right) \propto \vec{m} \end{cases} \text{ but } \begin{cases} -\vec{n} \prec \vec{n} - \left(\vec{a} + \vec{b}\right) \prec \vec{n} \\ -\vec{n} \prec \vec{a} - \vec{b} \prec \vec{n} \end{cases} . \tag{63}$$

From here we verify that as $\vec{n} \not\succeq \vec{m}, \exists j : n_j < m_j$ and $gcd(\vec{m}) = 1$ and therefore no proportionality can be found. □

D QFI Matrix for Arbitrary States

Starting from the definition of an arbitrary pure state of Eq. 25 can write the elements of the QFI matrix (see Eq. 6) as:

$$\mathcal{Q}_{\mu\nu}(\rho_{\boldsymbol{\theta}}) = 4\mathrm{Re}\left\{\sum_{l,m=1}^{2^n}\alpha_l^*\alpha_m\left\langle\mathcal{G}_l|\boldsymbol{G}_\mu\boldsymbol{G}_\nu|\mathcal{G}_m\right\rangle - \sum_{l,m=1}^{2^n}\alpha_l^*\alpha_m\left\langle\mathcal{G}_l|\boldsymbol{G}_\mu|\mathcal{G}_m\right\rangle\sum_{p,q=1}^{2^n}\alpha_p^*\alpha_q\left\langle\mathcal{G}_p|\boldsymbol{G}_\nu|\mathcal{G}_q\right\rangle\right\}, \tag{64}$$

with $\boldsymbol{G}_\mu = \sum_{j\in\mu} G_j$. To calculate the different elements above consider the following labeling for the basis states: let $\tilde{s}_l^\pm = (G_1^\perp)^{l_1}\otimes(G_2^\perp)^{l_2}\otimes\cdots\otimes(G_{n-1}^\perp)^{l_{n-1}}\otimes(G_n)^\pm$, where $G_n^+ = \mathbb{1}$ and $G_n^- = G_n$. Let $l\in\{0,1,\cdots,2^{n-1}-1\}$ and $l_1l_2\cdots l_{n-1}$ be the binary string associated to l. From our definition of $G, G^\perp$, we also have that:

$$\begin{aligned} G_j\circ G_j^\perp\circ G_j &= -G_j^\perp, \qquad & G_j\circ G_j\circ G_j &= G_j,\\ G_j^\perp\circ G_j\circ G_j^\perp &= -G_j, \qquad & G_j^\perp\circ G_j^\perp\circ G_j^\perp &= G_j^\perp. \end{aligned} \tag{65}$$

Using this when applying $\tilde{s}_l^\pm$ to the stabilizer table in Eq. 22, we get a minus sign for the lines j such that $l_j = 1$. This yields:

$$\begin{aligned} \left\langle\mathcal{G}_l^\pm\right|\sum_{j\in\mu}\sum_{k\in\nu}G_jG_k\left|\mathcal{G}_m^\pm\right\rangle &= h_{\mathcal{N}_\mu}^*(l)h_{\mathcal{N}_\nu}^*(m)\left\langle\mathcal{G}_l^\pm|\mathcal{G}_m^\pm\right\rangle\\ \left\langle\mathcal{G}_l^\pm\right|\sum_{j\in\mu}G_j\left|\mathcal{G}_m^\pm\right\rangle &= h_{\mathcal{N}_\mu}^*(l)\left\langle\mathcal{G}_l^\pm|\mathcal{G}_m^\mp\right\rangle, \end{aligned} \tag{66}$$

where $h_{\mathcal{N}_\mu}^*$ is the μ element of the vector-Hamming weight in Def. 3.3. Note that states differing on $\pm$ have the same Hamming-weight, as expected since G_n commutes with all G_jG_k terms. We can rewrite then Eq. 64 the QFI in the following way:

$$\begin{aligned} \mathcal{Q}_{\mu\nu}(\rho_{\boldsymbol{\theta}}) &= \sum_{l=0}^{2^{n-1}-1}\left[|\alpha_l^+|^2+|\alpha_l^-|^2\right]h_{\mathcal{N}_\mu}^*(l)h_{\mathcal{N}_\nu}^*(l) -\\ &- \left[\sum_{l=0}^{2^{n-1}-1}2\mathrm{Re}\left\{\alpha_l^{+^*}\alpha_l^-\right\}h_{\mathcal{N}_\mu}^*(l)\right]\left[\sum_{q=0}^{2^{n-1}-1}2\mathrm{Re}\left\{\alpha_q^{+^*}\alpha_q^-\right\}h_{\mathcal{N}_\nu}^*(q)\right]\\ &= \sum_l\lambda_l h_{\mathcal{N}_\mu}^*(l)h_{\mathcal{N}_\nu}^*(l) - \left[\sum_l v_l h_{\mathcal{N}_\mu}^*(l)\right]\left[\sum_q v_q h_{\mathcal{N}_\nu}^*(q)\right]. \end{aligned} \tag{67}$$

Let $\boldsymbol{\mathcal{N}} = \{\mathcal{N}_\mu\}_{\mu\in V}$ be the partition of the set of qubits into each of the nodes. Assembling the last equation for all entries $\mu\nu$ we get exactly:

$$\begin{aligned} \boldsymbol{\mathcal{Q}}(\rho_{\boldsymbol{\theta}}) &= \sum_m\lambda_m\vec{h}_{\boldsymbol{\mathcal{N}}}^*(m)\vec{h}_{\boldsymbol{\mathcal{N}}}^{*^T}(m) - \sum_m v_m\vec{h}_{\boldsymbol{\mathcal{N}}}^*(m)\sum_q v_q\vec{h}_{\boldsymbol{\mathcal{N}}}^{*^T}(q)\\ &= \sum_{m,q}\mathfrak{Q}_{mq}\vec{h}_{\boldsymbol{\mathcal{N}}}^*(m)\vec{h}_{\boldsymbol{\mathcal{N}}}^*(q)^T\\ &= C\mathfrak{Q}C^T, \end{aligned} \tag{68}$$

where C is a matrix where each line is given by a vector $\vec{n}-2\vec{c}_i$, where $\vec{0}\preceq\vec{c}_i\prec\vec{n}$. This is equivalent, under the choice of $G = Z, G^\perp = X$ to the GHZ state on n qubits, and the basis formed by $|\mathcal{G}_m^\pm\rangle\propto|m\rangle\pm|\overline{m}\rangle$ where m ranges between 0 and $2^{n-1}-1\equiv N$, is represented by the binary string associated to the number m and $\overline{m}$ is the binary negation of m (*e.g.* $m = 00101, \overline{m} = 11010$). Furthermore, we also get two additional important properties:

from Eq. 68 we can see that the QFI matrix can be decomposed in $\mathfrak{Q} = \Lambda - \vec{v}\vec{v}^T$, where $\Lambda = diag(\lambda_0, ..., \lambda_m, ..., \lambda_N)$ and $\vec{v} = (v_0, ..., v_m, ..., v_N)$. On top of this, we can verify that:

$$|\alpha_j^+ \pm \alpha_j^-|^2 \geq 0 \implies |\alpha_j^+|^2 + |\alpha_j^-|^2 \geq \pm 2\mathrm{Re}\left\{\alpha_j^+ \alpha_j^{-*}\right\} \implies \lambda_j \geq |v_j|. \tag{69}$$

E Matrix Rank Inequalities

Let us introduce some additional theorems regarding symmetric real matrices, which are the ones resultant from our problem. We start by the following theorem, which allows us to pick one and only one subspace in the set of states we can choose to construct a private state:

Theorem E.1. *Let $A \in \mathbb{R}^{n\times n}$ be a symmetric matrix given by $A = \Lambda - \vec{v}\vec{v}^T$, where Λ is a diagonal matrix with all entries real and non-negative summing to 1 and $\vec{v}$ is a vector in $\mathbb{R}^n$ such that $\|\vec{v}\| \leq 1$ and in particular $\forall i \in \{1, \ldots, n\} : \lambda_i \geq |v_i|$. A is positive semi-definite and the rank of A is at least*

$$rank\ \Lambda \geq rank\ A \geq rank\ \Lambda - 1,$$

and $rank\ A = rank\ \Lambda - 1$ iff. $\lambda_j = |v_j|$, $\forall j$.

Proof. We start by reducing the problem into considering only the non-zero entries of Λ and $\vec{v}$, as all the zero entries of Λ do not contribute for the rank and the zero entries of $\vec{v}$ have corresponding values in Λ which are already eigenvalues of A. Also, we can never have a non-zero entry in $\vec{v}$ associated to a zero value in Λ, from the conditions stated. Denote the vector $\vec{\lambda}$ as the vector of all the positive diagonal values of Λ. The condition imposed on $\vec{v}$ means that $\forall i \in \{1, \ldots, n\} : \lambda_i \geq |v_i|$, which allows us to say:

$$\begin{gathered}\forall \vec{y} \neq \vec{0}\ , \exists\ \vec{x} \neq \vec{0} : \vec{y}^T\left(\Lambda - \vec{v}\vec{v}^T\right)\vec{y} \geq \vec{x}^T\left(\Lambda - \vec{\lambda}\vec{\lambda}^T\right)\vec{x} \\ \vec{y}^T A \vec{y} \geq \vec{x}^T B \vec{x}.\end{gathered} \tag{70}$$

In particular, one could consider the vector $\vec{x}$ where $(\vec{x})_j = |(\vec{y})_j|$. By doing this, we can find bound the eigenvalues of A.

$$\begin{aligned}\vec{x}^T\left(\mathrm{diag}(\vec{\lambda}) - \vec{\lambda}\vec{\lambda}^T\right)\vec{x} &= \sum_i x_i^2\lambda_i - (\sum_i x_i\lambda_i)^2 \\ &= \sum_i x_i^2\lambda_i - (\sum_i x_i\lambda_i)(\sum_j x_j\lambda_j) \\ &= \sum_i x_i^2\lambda_i(1-\lambda_i) - \sum_{i,j\neq i} x_i\lambda_i x_j\lambda_j \\ &= \sum_i x_i^2\lambda_i \sum_{j\neq i}\lambda_j - 2\sum_{i,j>i} x_i\lambda_i x_j\lambda_j \\ &= \sum_i\sum_{j>i}\lambda_i\lambda_j(x_i^2 - 2x_ix_j + x_j^2) \\ &= \sum_i\sum_{j>i}\lambda_i\lambda_j(x_i - x_j)^2.\end{aligned} \tag{71}$$

Since each λ_i is by construction positive and non-zero, this means this expression is always positive, and is only zero when $(x_i - x_j)^2 = 0\ \forall i, j$, which only happens for the null vector $\vec{0}$ and the $\vec{1}/\sqrt{n}$.

Suppose $\exists j : \lambda_j > |v_j|$. In this case, Eq. 70 is never saturated, unless $(\vec{y})_j$ is zero, which implies $\vec{x}^T B \vec{x} > 0$. This means A is definite positive, and consequently that it has the rank of Λ. The other possible case is if $\forall\ j : \lambda_j = |v_j|$. Consider the matrix $D = diag((\vec{v})_j/|(\vec{v})_j|)$ which transforms $\vec{v} \to \vec{\lambda}$, $D\vec{v} = \vec{\lambda}$. Notice this matrix is a change of basis as $DD^T = \mathbb{1}$ and moreover that $DAD^T = B$ in this case. This allows us to map the eigenvectors of B into the eigenvectors of A, proving the lower bound on the rank, as $\vec{1}/\sqrt{n}$ is the only non-zero vector than spans the null space of B. This means the rank of A is bounded between the rank of Λ and rank Λ -1, where the latest equality only happens iff. $\forall\ j : \lambda_j = |v_j|$. □

Proposition E.1. *Let $A \in \mathbb{R}^{n\times n}$ be symmetric and $B \in \mathbb{R}^{k\times n}$. If A has full rank, then BAB^T has rank equal to the rank of B.*

$$rank\ A = n \quad \implies \quad rank\ BAB^T = rank\ B$$

Proof. Since A is symmetric, consider its diagonalization $A = Q\Lambda Q^T$.

$$BAB^T = BQ\Lambda Q^T B^T = BQ\sqrt{\Lambda}Q^T Q\sqrt{\Lambda}Q^T B^T = \tilde{B}\tilde{B}^T \implies \text{rank}\ \tilde{B}\tilde{B}^T = \text{rank}\tilde{B} = \text{rank}B,$$

where used properties of the rank, namely, $\text{rank}BB^T = \text{rank}B^T B = \text{rank}B = \text{rank}B^T$ and if A is a $l \times m$ matrix with rank m and B is a $m \times n$ matrix, $\text{rank}AB = \text{rank}B$. □

Proposition E.2. *Let $A \in \mathbb{R}^{n\times n}$ be symmetric and $B \in \mathbb{R}^{k\times n}$. If A has rank $n-1$, then:*

$$rank\ A = n - 1 \quad \implies \quad rank\ B \geq rank\ BAB^T \geq rank\ B - 1.$$

Proof. Consider the same as before, but in the last step apply the Sylvester inequality for the rank of $\sqrt{A}B$:

$$\text{rank}\ B \geq \min\{\text{rank}\ \sqrt{A}, \text{rank}\ B\} \geq \text{rank}\ \tilde{B} \geq \text{rank}\ B + \text{rank}\ \sqrt{A} - n = \text{rank}\ B - 1.$$

□

Proposition E.3. *Let V, W be two vector spaces. Let V_1 and V_2 be two $m \times n$ matrices with vectors in V. If $\mathsf{span}(V_1) = \mathsf{span}(V_2)$ then $\mathsf{span}(V_1 W_1) = \mathsf{span}(V_2 W_1)$ for any $n \times p$ matrix W_1 with vectors in W.*

Proof. If $\mathsf{span}(V_1) = \mathsf{span}(V_2)$ then $\exists Q : V_2 = QV_1$ and is invertible. The proof concludes by realising that $\mathsf{span}(QA) = \mathsf{span}(A)$ for any invertible Q, given the definition of a span of a set of vectors. □

F Private States - Proofs

Theorem 3.4 (Minimal privacy zone)**.** *Let $\vec{a}, \vec{n} \in \mathbb{Z}^k$, $gcd(\vec{a}) = 1$ and $f(\boldsymbol{\theta})$ be the linear function given by $f(\boldsymbol{\theta}) = \vec{a} \cdot \vec{\boldsymbol{\theta}}$. Then, there is only one family of pure states that is capable of estimating privately the function f using $\vec{n} = \vec{a}$ distributed resources and access to local separable dynamics $U_{\boldsymbol{\theta}}$.*

$$F_{GHZ} = \{\alpha\,|0\rangle^{\otimes n} + \beta\,|1\rangle^{\otimes n} : \alpha, \beta \in \mathbb{C} \setminus \{0\}, |\alpha|^2 + |\beta|^2 = 1\}$$

$$\mathcal{P}(\mathcal{Q}(U_{\boldsymbol{\theta}}\,|\psi\rangle), \vec{a}) = 1 \quad \iff \quad \exists U \in LU : U\,|\psi\rangle \in F_{GHZ}$$

Proof. The proof in the indirect way comes trivially from calculating the privacy for the family of states F_{GHZ}, together with Corol. 2.1, we get that difference up to a LU operation. Doing the same as before, now we have a different $\mathfrak{Q}$ and C matrices, as $\vec{n} = \vec{a}$. When looking at the matrix $\mathfrak{Q}$ note that the first coefficient λ_0 and v_0 are associated with the span of the family of states F_{GHZ}, as by varying them, we get all the states in F_{GHZ}. Doing the same analysis as before, we get that now $\vec{a} \in C$ and $dim_{\vec{a}}(C) = 1$, *i.e.* it only appears once in the lines of C. Constructing the same table to analyze privacy:

rank supp $\mathfrak{Q}$	rank $C_{\text{supp}\,\mathfrak{Q}}$	rank $C\mathfrak{Q}C^T$	Reasoning	Privacy
any	1	≤ 1	Trivial	Iff. $C_{\text{supp}\,\mathfrak{Q}} = \vec{a}$
dim supp $\mathfrak{Q}$	≥ 2	≥ 2	Prop. E.1	Never
dim supp $\mathfrak{Q}$-1	2	1 or 2	Prop. E.2	Check
dim supp $\mathfrak{Q}$-1	> 2	> 1	Prop. E.2	Never

Checking again the case of rank supp $\mathfrak{Q}$ = dim supp $\mathfrak{Q} - 1$ with rank $C_{\text{supp}\,\mathfrak{Q}} = 2$. Using the same reasoning we find a vector $D\vec{w}$ in the orthogonal subspace of $D\vec{1}$, $\mathsf{span}P^{\perp}$, acting on two different lines of $C_{\text{supp}\,\mathfrak{Q}}$:

$$\begin{aligned} D\vec{w}C_{\text{supp}\,\mathfrak{Q}} &= 1/\sqrt{2}\left(\vec{h}^*_{\boldsymbol{\mathcal{N}}}(i) \pm \vec{h}^*_{\boldsymbol{\mathcal{N}}}(j)\right) \\ &= \begin{cases} 2/\sqrt{2}\left[\vec{n} - \left(\vec{h}_{\boldsymbol{\mathcal{N}}}(i) + \vec{h}_{\boldsymbol{\mathcal{N}}}(j)\right)\right] \\ 2/\sqrt{2}\left(\vec{h}_{\boldsymbol{\mathcal{N}}}(i) - \vec{h}_{\boldsymbol{\mathcal{N}}}(j)\right) \end{cases} . \end{aligned} \tag{72}$$

From here there are two options:

(i) i or j correspond to the GHZ state, and in that case we have that $\vec{h}_{\boldsymbol{\mathcal{N}}}(i) \pm \vec{h}_{\boldsymbol{\mathcal{N}}}(j) = \vec{0} \equiv \vec{h}_{\boldsymbol{\mathcal{N}}}(j) = \vec{0}$, meaning that $i = j$ and contradicting rank-2 of $C_{\text{supp}\,\mathfrak{Q}}$;

(ii) neither i nor j correspond to the GHZ state, and we recover that $C_{\text{supp}\,\mathfrak{Q}}$ only has vectors $\vec{c}_i \prec \vec{a}$, which is the case for the non-existence of a private state.

This means also this case is never private. Consequently, the only private state is the one spanned by a matrix with a unique non-zero entry correspondent to $\lambda_0 - v_0^2$. Moreover, this is maximized for $v_0^2 = 0$, meaning a perfect GHZ state, up to a LU operation.

□

Proposition 3.7. *All families of pure states $\mathcal{F}(\boldsymbol{\mathcal{N}}, \vec{a}, \vec{d})$, are capable of estimating privately the function $f(\boldsymbol{\theta}) = \vec{a} \cdot \vec{\boldsymbol{\theta}}$ using $\vec{n} = \vec{a} + \vec{b}$ distributed resources.*

Proof. This is a direct consequence of the invariance of the Hamming-weight introduced in Props. 3.1,3.2. Looking at the terms that appear in the QFI, fix the encoding dynamics basis at Z, as we have chosen our distributed s-states (Def. 3.5) in the computational basis. Notice this does not affect the generality of our proof, as again we are always an LU operation from any other basis (Corol. 2.1). Using this fact, and the fact that the vectorial Hamming-weight is invariant under the distributed permutations, we get that:

$$\begin{aligned} \sum_{j\in\mu} Z_j \left|\psi\right\rangle &= h_{\mathcal{N}_\mu}(\left|s(b_{1\mu}, a_\mu + b_{0\mu})\right\rangle) \left|\psi\right\rangle = (a_\mu + b_{0\mu} - b_{1\mu}) \left|\psi\right\rangle , \\ \sum_{j\in\mu} Z_j \left|\tilde{\psi}\right\rangle &= h_{\mathcal{N}_\mu}(\left|s(a_\mu + b_{1\mu}, b_{0\mu})\right\rangle) \left|\tilde{\psi}\right\rangle = (-a_\mu + b_{0\mu} - b_{1\mu}) \left|\tilde{\psi}\right\rangle , \end{aligned} \tag{73}$$

Where we used that $\vec{b} = \vec{b}_0 + \vec{b}_1$ which correspond to the amount of 0's and 1's respectively. Note that $\vec{d} = \vec{b}_1$ as well. After assembling in the QFI matrix we get:

$$\boldsymbol{\mathcal{Q}} = \vec{a}\vec{a}^T \left[|\alpha^2| + |\beta|^2 - (|\alpha|^2 - |\beta|^2)^2 \right], \tag{74}$$

which means private. Moreover, it is maximised for $|\alpha| = |\beta|$. □

Theorem 3.5 (Minimal Plus Ancilla Zone)**.** *Let $\vec{a}, \vec{b}, \vec{n} \in \mathbb{Z}^k$, $gcd(\vec{a}) = 1$ and $f(\boldsymbol{\theta})$ be the linear function given by $f(\boldsymbol{\theta}) = \vec{a} \cdot \vec{\boldsymbol{\theta}}$. Then, all pure states, up to LU, capable of estimating privately the function f using $\vec{n} = \vec{a} + \vec{b}$ distributed resources and access to local separable dynamics $U_{\boldsymbol{\theta}}$, belong a family of the set of $\vec{a}$-Private-Ancilla States introduced in Def. 3.6.*

$$\mathcal{P}(\mathcal{Q}(U_{\boldsymbol{\theta}} |\psi\rangle), \vec{a}) = 1 \quad \iff \quad \exists U \in LU, \vec{d} \in \mathbb{N}_0^k, \vec{0} \preceq \vec{d} \preceq \vec{n} - \vec{a} : U |\psi\rangle \in \mathcal{F}(\boldsymbol{\mathcal{N}}, \vec{a}, \vec{d})$$

Proof. The inverse direction is a direct consequence from Thm. 3.7. The direct proof comes again from the QFI. Construct the same decomposition into $C\mathfrak{Q}C^T$ as before, where the basis of $\mathfrak{Q}$ are the families correspondent to $\boldsymbol{F}_{GHZ}$.

rank supp $\mathfrak{Q}$	rank $C_{\text{supp}\,\mathfrak{Q}}$	rank $C\mathfrak{Q}C^T$	Reasoning	Privacy
any	1	≤ 1	Trivial	Iff. $C_{\text{supp}\,\mathfrak{Q}} = \vec{a}$
dim supp $\mathfrak{Q}$	≥ 2	≥ 2	Prop. E.1	Never
dim supp $\mathfrak{Q}$-1	2	1 or 2	Prop. E.2	Check
dim supp $\mathfrak{Q}$-1	> 2	> 1	Prop. E.2	Never

Now, for the first time we have that $\dim\{\vec{c}_j \in C : \vec{c}_j = \vec{a}\} \equiv \mathfrak{Q}_{\vec{a}}$ is either 0 or larger than 1. It is larger than 1 if $\vec{b} = \vec{n} - \vec{a}$ has all entries divisible by two, and one can find the family of states such that $\vec{b}_0 = \vec{b}_1$. This is a consequence of the symmetric Hamming weight that remains the same when adding the same amount of 0s and 1s to a bitstring.

Looking at the case of rank supp $\mathfrak{Q}$ = dim supp $\mathfrak{Q}$ − 1 with rank $C_{\text{supp}\,\mathfrak{Q}} = 2$, we can find a way to construct all the others families. Using the same reasoning as before, let D be the matrix such that $D\vec{1}$ spans the null space of $\boldsymbol{\mathcal{Q}}$. Denote the orthogonal space of this vector by $P^{\perp}$. Let W be the set of vectors given by $W^{\pm} = \{w | w = \vec{e}_i \pm \vec{e}_j, \text{sign}(D_{ii}) = \mp\text{sign}(D_{jj})\}$, and Prop. E.3 allows us to use this vectors to continue our proof, as $\mathsf{span}(P^{\perp}) = \mathsf{span}(W^+ \cup W^-)$. Looking first at W^-,the options let us check which vectors $\vec{c}_i - \vec{c}_j$ are proportional to $\vec{a}$:

$$\begin{aligned} \vec{h}^*_{\boldsymbol{\mathcal{N}}}(i) - \vec{h}^*_{\boldsymbol{\mathcal{N}}}(j) &= \delta\vec{a}, \qquad \delta = \{\pm 1, \pm 2\} \\ \vec{n} - 2\vec{h}_{\boldsymbol{\mathcal{N}}}(i) - \left(\vec{n} - 2\vec{h}_{\boldsymbol{\mathcal{N}}}(j)\right) &= \delta\vec{a}, \qquad \delta = \{\pm 1, \pm 2\} \\ \vec{h}_{\boldsymbol{\mathcal{N}}}(i) - \vec{h}_{\boldsymbol{\mathcal{N}}}(j) &= \tilde{\delta}\vec{a}, \qquad \tilde{\delta} = \{\pm 1\} \\ \implies \vec{h}_{\boldsymbol{\mathcal{N}}}(i) = \vec{a} + \vec{b}_j \wedge \vec{h}_{\boldsymbol{\mathcal{N}}}(j) &= \vec{b}_j, \end{aligned} \tag{75}$$

where we used the fact that $\vec{h}_{\boldsymbol{\mathcal{N}}}(\cdot)$, is an positive integer vector and $gcd(\vec{a}) = 1$. Moreover, we introduce the notation $\vec{b}_i$ as a vector between $\vec{0} \preceq \vec{b}_i \prec \vec{b}$. Substituting for $\vec{h}^*_{\boldsymbol{\mathcal{N}}}(i)$ and $\vec{h}^*_{\boldsymbol{\mathcal{N}}}(j)$ and using $\vec{b}_i = \vec{b} - \vec{b}_j$ we observe:

$$\begin{aligned} \vec{h}^*_{\boldsymbol{\mathcal{N}}}(i) &= \vec{n} - 2(\vec{a} + \vec{b}_j) = \vec{a} + \vec{b} - 2(\vec{a} + \vec{b}_j) = -\vec{a} + \vec{b} - 2\vec{b}_j = -(\vec{a} + \vec{b} - 2\vec{b}_i) = -(\vec{n} - 2\vec{b}_i) \\ \vec{h}^*_{\boldsymbol{\mathcal{N}}}(j) &= \vec{n} - 2\vec{b}_j = \vec{a} + \vec{b} - 2\vec{b}_j. \end{aligned} \tag{76}$$

The equations for the subspace W^+ are:

$$\begin{aligned}
\vec{h}^*_{\boldsymbol{\mathcal{N}}}(i) + \vec{h}^*_{\boldsymbol{\mathcal{N}}}(j) &= \delta\vec{a}, \qquad \delta = \{0, \pm 1, \pm 2\} \\
\vec{n} - 2\vec{h}_{\boldsymbol{\mathcal{N}}}(i) + \left(\vec{n} - 2\vec{h}_{\boldsymbol{\mathcal{N}}}(j)\right) &= \delta\vec{a}, \qquad \delta = \{0, \pm 1, \pm 2\} \\
\vec{n} - \left(\vec{h}_{\boldsymbol{\mathcal{N}}}(i) + \vec{h}_{\boldsymbol{\mathcal{N}}}(j)\right) &= \tilde{\delta}\vec{a}, \qquad \tilde{\delta} = \{0, \pm 1\} \\
\implies \left(\vec{h}_{\boldsymbol{\mathcal{N}}}(i) + \vec{h}_{\boldsymbol{\mathcal{N}}}(j) = \vec{a} + \vec{b}\right) &\vee \left(\vec{h}_{\boldsymbol{\mathcal{N}}}(i) + \vec{h}_{\boldsymbol{\mathcal{N}}}(j) = \vec{b}\right) \vee \left(\vec{h}_{\boldsymbol{\mathcal{N}}}(i) + \vec{h}_{\boldsymbol{\mathcal{N}}}(j) = 2\vec{a} + \vec{b}\right).
\end{aligned} \tag{77}$$

This means the overall solution are the vectors inside $C_{\mathrm{supp}\,\mathfrak{Q}}$, such that:

$$\begin{cases} \vec{c}_i = \vec{n} - 2\left(\vec{a} + \vec{b}_i\right) \vee \vec{c}_i = \vec{n} - 2\vec{b}_i, \\ \vec{c}_j = \vec{n} - 2\left(\vec{a} + \vec{b}_j\right) \vee \vec{c}_j = \vec{n} - 2\vec{b}_j, \end{cases}, \qquad \vec{b}_i + \vec{b}_j = \vec{b}. \tag{78}$$

Substituting we actually see that $\vec{n} - 2\left(\vec{a} + \vec{b}_i\right) = -(\vec{n} - 2\vec{b}_j)$, meaning they are in fact spanned by a state in the same family (see Prop. F.2). This means choosing only the combination $\vec{c}_i = \vec{n} - 2\vec{b}_i \wedge \vec{c}_j = \vec{n} - 2\vec{b}_j$ is sufficient. The set of states with the same vectorial Hamming-weight, are exactly the states belonging to the equivalence class, by definition. From the construction of matrix $\mathfrak{Q}$, we get that each line is associated with the following family of states:

$$\begin{aligned}
&\overline{F}_{GHZ_m} = \left\{\alpha\left|m\right\rangle + \beta\left|\overline{m}\right\rangle, \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1\right\} \\
&\lambda_i = |\alpha_i|^2 + |\alpha_{i+1}|^2, v_i = 2\mathrm{Re}\left\{\alpha_i\alpha^*_{i+1}\right\}, \alpha = \frac{\alpha_i + \alpha_{i+1}}{\sqrt{2}}, \beta = \frac{\alpha_i - \alpha_{i+1}}{\sqrt{2}} \\
&\lambda_i = |v_i| \implies \begin{cases} \alpha = 1, \beta = 0, v_i/|v_i| = 1 \\ \alpha = 0, \beta = 1, v_i/|v_i| = -1 \end{cases}.
\end{aligned} \tag{79}$$

This means we can only take states i such that, up to permutation of qubits (see Prop. F.1), that have $\vec{h}_{\boldsymbol{\mathcal{N}}}(i) = \vec{b}_i$, together with states j that $\vec{h}_{\boldsymbol{\mathcal{N}}}(\bar{j}) = \vec{a} + \vec{b}_j$. Given that we can only choose $\vec{b}_i, \vec{b}_j$ such that $\vec{b}_i + \vec{b}_j = \vec{b}$ (Eq. 78) and $\vec{h}_{\boldsymbol{\mathcal{N}}}(\bar{j}) = \vec{n} - \vec{h}_{\boldsymbol{\mathcal{N}}}(j) = \vec{n} - (\vec{a} + \vec{b}_j) = \vec{b} - \vec{b}_j$, then this are exactly the family of states given by $\mathcal{F}(\boldsymbol{\mathcal{N}}, \vec{a}, \vec{b}_i)$. By doing the same for each possible set of $\vec{b}_i, \vec{b}_j$, one generates each of the possible families of private states. Note however that one cannot create a superposition of states of different families, as that means the rank of $C_{\mathrm{supp}\,\mathfrak{Q}}$ would be larger than 2, which would always mean a non-private state (check table). Moreover, one recovers the fact that if $\vec{b}$ is divisible by 2, then for $\vec{b}_i = \vec{b}_j = \vec{b}/2$ is the case of a rank-1 $C_{\mathrm{supp}\,\mathfrak{Q}}$. Given that all other possibilities create either not rank-1 QFI matrices, or QFI matrices which are not proportional to $\vec{a}\vec{a}^T$, this are the only sets of private states. □

Below we provide two additional propositions that allowed some simplifications on the theorems above.

Proposition F.1. *Let $\sigma \in S_{\boldsymbol{\mathcal{N}}}$. Let $\left|GHZ_m\right\rangle = \alpha\left|m\right\rangle + \beta\left|\overline{m}\right\rangle$, where m is a binary string with length $\|\vec{n}\|_1$ and $\overline{(\cdot)}$ is the binary conjugation of $(\cdot)$.*

$$h_{\boldsymbol{\mathcal{N}}}(m) = h_{\boldsymbol{\mathcal{N}}}\left(\sigma(m)\right) \iff \mathcal{Q}(\left|GHZ_m\right\rangle) = \mathcal{Q}\left(\sigma(\left|GHZ_m\right\rangle)\right) \tag{80}$$

Proposition F.2. *Let $\left|GHZ_m\right\rangle = \alpha\left|m\right\rangle + \beta\left|\overline{m}\right\rangle$ and $\left|GHZ_{\overline{m}}\right\rangle = \alpha\left|\overline{m}\right\rangle + \beta\left|m\right\rangle$, where m is a binary string with length $\|\vec{n}\|_1$ and $\overline{(\cdot)}$ is the binary conjugation of $(\cdot)$.*

$$\mathcal{Q}(\left|GHZ_m\right\rangle) = \mathcal{Q}\left(\left|GHZ_{\overline{m}}\right\rangle\right) \tag{81}$$

Finally, the statement for when we have multiples of the vector of resources:

Theorem 3.6 (Multiple Privacy)**.** *All states which are described as a private logical state (Def. 3.7) define private states for quantum distributed sensing, up to LU operations.*

Proof. From Corol. 2.1 we get that we can fix dynamics as Z dynamics, without loosing any generality, and work with the regular computational basis for the qubits. This comprises the statement up to LU operations. Then, starting from:

$$\begin{aligned}\sum_{j\in l} Z_j \left|0_L\right\rangle_l \equiv \boldsymbol{Z}_\mu^l \left|0_L\right\rangle_l &= \left(a_\mu + b_{0_\mu}^l - b_{1_\mu}^l\right)\left|0_L\right\rangle = \left(a_\mu + \Delta b_\mu^l\right)\left|0_L\right\rangle, \\ \sum_{j\in l} Z_j \left|1_L\right\rangle_l \equiv \boldsymbol{Z}_\mu^l \left|1_L\right\rangle_l &= \left(-a_\mu + b_{0_\mu}^l - b_{1_\mu}^l\right)\left|1_L\right\rangle = \left(-a_\mu + \Delta b_\mu^l\right)\left|1_L\right\rangle,\end{aligned} \tag{82}$$

define $\left|j\right\rangle = \left|j_1 j_2 \cdots j_d\right\rangle$, such that $\boldsymbol{Z}_\mu^l \left|j_L\right\rangle_l = \left((-1)^{j_l} a_\mu + \Delta b_\mu^l\right)\left|j_L\right\rangle_l$ and note that:

$$\boldsymbol{Z}_\mu \left|j\right\rangle = \sum_{l=1}^{d} \boldsymbol{Z}_\mu^l \left|j\right\rangle = \left(h^*(j) a_\mu + \sum_{l=1}^{d} \Delta b_\mu^l\right)\left|j\right\rangle. \tag{83}$$

This means that, for $\left|\psi\right\rangle \in \mathfrak{F}$, the QFI will have the following form:

$$\begin{aligned}\mathcal{Q}_{\mu\nu} &\propto \left\langle\psi\right| \boldsymbol{Z}_\mu \boldsymbol{Z}_\nu \left|\psi\right\rangle - \left\langle\psi\right| \boldsymbol{Z}_\mu \left|\psi\right\rangle \left\langle\psi\right| \boldsymbol{Z}_\nu \left|\psi\right\rangle \\ &= \sum_{j,m=0}^{2^d-1} \alpha_j^* \alpha_m \left\langle j\right| \boldsymbol{Z}_\mu \boldsymbol{Z}_\nu \left|m\right\rangle - \sum_{j,m=0}^{2^d-1} \alpha_j^* \alpha_m \left\langle j\right| \boldsymbol{Z}_\mu \left|m\right\rangle \sum_{p,q=0}^{2^d-1} \alpha_p^* \alpha_q \left\langle p\right| \boldsymbol{Z}_\nu \left|k\right\rangle \\ &= \sum_{j=0}^{2^d-1} \left|\alpha_j\right|^2 \left(h^*(j) a_\mu + \sum_{l=1}^{d} \Delta b_\mu^l\right)\left(h^*(j) a_\nu + \sum_{l=1}^{d} \Delta b_\nu^l\right) \\ &\qquad - \sum_{j,p=0}^{2^d-1} \left|\alpha_j\right|^2 \left|\alpha_p\right|^2 \left(h^*(j) a_\mu + \sum_{l=1}^{d} \Delta b_\mu^l\right)\left(h^*(p) a_\nu + \sum_{l=1}^{d} \Delta b_\nu^l\right) \\ &= \left[\sum_{j=0}^{2^d-1} \left|\alpha_j\right|^2 h^*(j)^2 - \sum_{j,p=0}^{2^d-1} \left|\alpha_j\right|^2 \left|\alpha_p\right|^2 h^*(j) h^*(p)\right] a_\mu a_\nu,\end{aligned} \tag{84}$$

which makes the QFI matrix always proportional to $\vec{a}\vec{a}^T$, resulting always in a private state.

□

G Private States Existence for General Hamiltonians

Let us start by repeating and proving Thm. 3.7:

Theorem 3.7 (Existence of Private States)**.** *Let a distributed sensing scenario be governed by local encoding dynamics in the form of Eq. 7, with associated discrete subset $\mathcal{O}$. For each vector $\vec{a}$ belonging to the higher order discrete subset $\mathcal{O}_-^2$, one can find a private state with respect to the linear function $f(\boldsymbol{\theta}) = \vec{a}\cdot\vec{\boldsymbol{\theta}}$. Moreover, no vector outside the equivalence class of $\mathcal{O}_-^2$ has a private state.*

Proof. Given the rewriting of the QFI matrix in Eq. 31, we already now from Thm. E.1 that the rank of this matrix is given by the rank $\operatorname{supp}\mathfrak{Q} - 1$, similarly to what we have

done before. By choosing the orthogonal subspace to the null space of $\operatorname{supp}\mathfrak{Q}$ we realize that the span of this space is generated by the vectors in $W = \{w | w = \vec{e}_{\vec{i}} - \vec{e}_{\vec{j}}\}$. Note that $WC_{\operatorname{supp}\mathfrak{Q}}$ generates a space of vectors $\mathcal{C} = \{\vec{c} | \vec{c} = \vec{c}_{\vec{i}} - \vec{c}_{\vec{j}}, \vec{c}_{\vec{i}}, \vec{c}_{\vec{j}} \in \mathcal{O}\}$. This is exactly the higher order discrete subspace generated by $\mathcal{O}$, *i.e.* $\mathcal{C} \subsetneq \mathcal{O}^2_-$. This already proves the first part of the theorem about the existence of private states, by choosing states with $\alpha_{\vec{i}}, \alpha_{\vec{j}}$ to be the only non-zero terms, associated to vectors $\vec{c}_{\vec{i}} - \vec{c}_{\vec{j}} = \vec{a} \in \mathcal{O}^2_-$.

The fact that only vectors in the equivalence class of $\mathcal{O}^2_-$ have private states is a consequence of $\mathsf{span}(\mathcal{C}) = \{\alpha\vec{a}, \alpha \in \mathbb{R}\}$ in order for privacy to be verified. If $\alpha\vec{a} \notin \mathcal{O}^2_-$ than one cannot build $\mathsf{span}(\mathcal{C})$, as every $\vec{c}_{\vec{i}} - \vec{c}_{\vec{j}}$ has to be proportional to $\vec{a}$ and $\vec{c}_{\vec{i}}, \vec{c}_{\vec{j}}$ can only be chosen from $\mathcal{O}$. □

To prove Prop. 3.8 let us first introduce and prove some additional propositions that will allows us to prove it:

Proposition G.1. *Let $X \in \mathcal{P}_n$ be a Pauli string and $\mathcal{H} \subseteq \mathcal{P}_n$ a subset of Pauli strings. Define an Hamiltonian as $H = \sum_{P\in\mathcal{H}} c_P P$, where all $c_P \neq 0$. Then:*

$$[X, H]_\pm = 0 \Leftrightarrow [X, P]_\pm = 0, \quad \forall\ P \in \mathcal{H}.$$

Proof. The inverse implication comes trivially from the linearity of the (anti)commutator $[\cdot,\cdot]_\pm$. The direct implication comes as follows: divide $\mathcal{H}$ into two disjoint sets $\mathcal{H} = \mathcal{H}_+ \cup \mathcal{H}_-$ such that $[X, P]_\pm = 0,\ \forall\ P \in \mathcal{H}_\pm$. This is always possible given that two Pauli strings either commute or anticommute. Then:

$$\begin{aligned}
[X, H]_\pm &= \sum_{P\in\mathcal{H}} c_P [X, P]_\pm \\
&= \sum_{P\in\mathcal{H}_\pm} c_P [X, P]_\pm + \sum_{P\in\mathcal{H}_\mp} c_P [X, P]_\pm \\
&= 0 + \sum_{P\in\mathcal{H}_\mp} c_P [X, P]_\pm \\
&= 2 \sum_{P\in\mathcal{H}_\mp} c_P PX \\
&= 2 \sum_{\tilde{P}\in\mathcal{H}_\mp X} c_{\tilde{P}} \tilde{P},
\end{aligned}$$

which can only be zero if all $c_{\tilde{P}}$ are 0, as the set of Pauli strings generates a basis for complex matrices, leading to a contradiction. □

Proposition G.2. *Let $\mathcal{H} \subseteq \mathcal{P}_n$ be a subset of Pauli strings. Define an Hamiltonian as $H = \sum_{P\in\mathcal{H}} c_P P$, where all $c_P > 0$. Then:*

$$\exists X \in \mathcal{P}_n : \{X, H\} = 0 \Leftrightarrow \{\lambda_H\} = \{+\lambda_H\} \cup \{-\lambda_H\}$$

Meaning for each eigenvalue of the Hamiltonian H, λ_H, its symmetric counterpart, $-\lambda_H$, is also an eigenvalue of H.

Proof. The direct proof follows very simply. $X \in \mathcal{P}_n \implies X^2 = \mathbb{1}$.

$$\begin{aligned}
\det(H - \lambda\mathbb{1}) &= \det(H - \lambda\mathbb{1}) \det(X^2) \\
&= \det(X) \det(H - \lambda\mathbb{1}) \det(X) \\
&= \det(XHX - \lambda X\mathbb{1}X) \\
&= \det(-H - \lambda\mathbb{1}),
\end{aligned}$$

which means the eigenvalues admit solutions for $\det(H-\lambda\mathbb{1})$ and $\det(H+\lambda\mathbb{1})$ and therefore if $\lambda_H \in \text{ev}$, $-\lambda_H \in \text{ev}$. The inverse proof comes as a consequence of the Pauli strings forming a basis for the space of complex matrices $\mathbb{C}^{2^n} \times \mathbb{C}^{2^n}$. Take U to be a unitary operation that switches from positive eigenstates to the negative ones: $U|\lambda_H^{\pm}\rangle = |\lambda_H^{\mp}\rangle$. Then:

$$\begin{aligned} UH|\lambda_H^{\pm}\rangle &= \pm\lambda_H U|\lambda_H^{\pm}\rangle = \pm\lambda_H|\lambda_H^{\mp}\rangle \\ HU|\lambda_H^{\pm}\rangle &= H|\lambda_H^{\mp}\rangle = \mp\lambda_H|\lambda_H^{\mp}\rangle \\ &\implies (UH+HU)|\lambda_H^{\pm}\rangle = 0, \quad \forall\ |\lambda_H^{\pm}\rangle, \end{aligned}$$

which means there is a unitary satisfying the anti-commutation relation. Given that U is a complex matrix, one can find a decomposition in terms of Pauli strings. Using Prop. G.1 and similar arguments for the proof of Prop. G.1, then one has to choose the decomposition among the set of anti-commuting Pauli strings only. This consequently means there is at least one Pauli string that anti-commutes with the Hamiltonian. □

This allows us to prove Prop. 3.8:

Proposition 3.8. *Let $\{\boldsymbol{H}_\mu\}_{\mu\in V}$ be the Hamiltonians describing some local general encoding dynamics.*

$$\forall\ \mu \in V\ \exists\ X_\mu \in \mathbb{1}\otimes\mathcal{P}_\mu : \{X_\mu, \boldsymbol{H}_\mu\} = 0 \implies \mathcal{O} \subsetneq \mathcal{O}_-^2 \tag{33}$$

Where $\mathbb{1}\otimes\mathcal{P}_\mu$ are the Pauli strings where only the elements in μ can be non-identity. This means the functions in $\mathcal{O}$ are available privately by choosing an appropriate state.

Proof. Follows directly from Prop. G.2. The stated conditions for each local Hamiltonian imply that the local eigenvalues λ_μ belong to a set such that if $+\lambda$ exists so does $-\lambda$. This means that if the vector $\vec{c}_i$ belongs to the discrete subset $\mathcal{O}$, so does the vector $-\vec{c}_i$. This consequently means that $\mathcal{O}_-^2$ where the vectors are built from $\vec{c}_i - \vec{c}_j$ will, in particular, include the vectors $\vec{c}_i - (-\vec{c}_i) = 2\vec{c}_i$. So $\mathcal{O} \sim 2\mathcal{O} \subseteq \mathcal{O}_-^2 \equiv \mathcal{O} \subsetneq \mathcal{O}_-^2$. □

Finally, we are able to prove Corol. 3.1:

Corollary 3.1 (Information Concentration)**.** *Given a distributed sensing scenario governed by local encoding dynamics in the form of Eq. 7, the maximum information extractable, given by functions of parameters in the vertices of $\overline{\mathcal{O}}_-^2$, is accessible only by a private state.*

Proof. This is a consequence of the decomposition of $\mathcal{Q} = C\mathfrak{Q}C^T$ of Eq. 31 and the fact that $\|\vec{a}\|_2$ is maximum for $\vec{a} \in V(\overline{\mathcal{O}}_-^2)$. Among only the private states, $\vec{a} \in \overline{\mathcal{O}}_-^2$, one can calculate the maximal QFI as:

$$\max \mathcal{Q}(\vec{a}) = \max \vec{a}^T\mathcal{Q}\vec{a} = \|\vec{a}\|_2^2 = \|\vec{c}_i - \vec{c}_j\|_2^2.$$

The privacy measure already incapsulates the fact that any private state will maximise information about the target function. This means the maximum information one can get about the maximum function is necessarily private. □

H QFI for Mixed States - Derivations

As said in the main text, to find the expression for the QFI in the mixed state case, we start by the most elementar expression for the QFI:

$$\mathcal{Q}_{\mu\nu}(\rho_{\boldsymbol{\theta}}) = \operatorname{Tr} \mathcal{R}_{\rho_{\boldsymbol{\theta}}}^{-1}(\partial_{\theta_\mu}\rho_{\boldsymbol{\theta}})\rho_{\boldsymbol{\theta}}\mathcal{R}_{\rho_{\boldsymbol{\theta}}}^{-1}(\partial_{\theta_\nu}\rho_{\boldsymbol{\theta}}). \tag{85}$$

Under the assumptions of the main text regarding the superoperator $\mathcal{R}_{\rho_{\boldsymbol{\theta}}}$, which corresponds to the symmetric logarithmic derivative, we can derive it in terms of the density matrix eigenvectors:

$$\mathcal{R}_{\rho}^{-1}(\partial_{\theta_\mu}\rho_{\boldsymbol{\theta}}) = \sum_{j,k} \frac{2}{\lambda_j + \lambda_k} \langle \mathcal{G}_j | \, \partial_{\theta_\mu}\rho_{\boldsymbol{\theta}} \, | \mathcal{G}_k \rangle \, | \mathcal{G}_j \rangle\langle \mathcal{G}_k | \, . \tag{86}$$

Using the notation $|\mathcal{G}'_k\rangle = U_{\boldsymbol{\theta}} \, |\mathcal{G}_k\rangle$:

$$\begin{aligned} \partial_{\theta_\mu}\rho_{\boldsymbol{\theta}} &= \partial_{\theta_\mu} \sum_{k\in\text{supp}} \lambda_k \, |\mathcal{G}'_k\rangle\langle\mathcal{G}'_k| \\ &= \sum_{k\in\text{supp}} \lambda_k \left[|\partial_{\theta_\mu}\mathcal{G}'_k\rangle\langle\mathcal{G}'_k| + |\mathcal{G}'_k\rangle\langle\partial_{\theta_\mu}\mathcal{G}'_k| \right], \end{aligned} \tag{87}$$

where we assumed that the encoding is unitary and done over the density matrix.

$$\begin{aligned} D^{\mu}_{ij} \equiv \langle \mathcal{G}'_i | \, \partial_{\theta_\mu}\rho_{\boldsymbol{\theta}} \, | \mathcal{G}'_j \rangle &= \langle \mathcal{G}'_i | \sum_k \lambda_k \left[|\partial_{\theta_\mu}\mathcal{G}'_k\rangle\langle\mathcal{G}'_k| + |\mathcal{G}'_k\rangle\langle\partial_{\theta_\mu}\mathcal{G}'_k| \right] |\mathcal{G}'_j\rangle \\ &= \sum_k \lambda_k \left[\langle \mathcal{G}'_i | \partial_{\theta_\mu}\mathcal{G}'_k\rangle \, \delta_{kj} + \delta_{ik} \, \langle \partial_{\theta_\mu}\mathcal{G}'_k | \mathcal{G}'_j\rangle \right] \\ &= \mathrm{id}_{\text{supp}}(j)\lambda_j \, \langle \mathcal{G}'_i | \partial_{\theta_\mu}\mathcal{G}'_j\rangle + \mathrm{id}_{\text{supp}}(i)\lambda_i \, \langle \partial_{\theta_\mu}\mathcal{G}'_i | \mathcal{G}'_j\rangle \\ &= [\mathrm{id}_{\text{supp}}(i)\lambda_i - \mathrm{id}_{\text{supp}}(j)\lambda_j] \, \langle \partial_{\theta_\mu}\mathcal{G}'_i | \mathcal{G}'_j\rangle \, , \end{aligned} \tag{88}$$

where the last step was taking into consideration that:

$$\begin{aligned} \partial_{\theta_\mu}(\langle \mathcal{G}'_i | \mathcal{G}'_j\rangle) = \partial_{\theta_\mu}(\langle \mathcal{G}_i | \mathcal{G}_j\rangle) = \partial_{\theta_\mu}(\delta_{ij}) &= 0 \\ &= \langle \partial_{\theta_\mu}\mathcal{G}'_i | \mathcal{G}'_j\rangle + \langle \mathcal{G}'_i | \partial_{\theta_\mu}\mathcal{G}'_j\rangle \, . \end{aligned} \tag{89}$$

Plugging it in the QFI we get that:

$$
\begin{aligned}
\mathcal{Q}_{\mu\nu}(\rho_{\boldsymbol{\theta}}) &= \mathrm{Tr}\left[\mathcal{R}_{\rho_{\boldsymbol{\theta}}}^{-1}(\partial_{\theta_\mu}\rho_{\boldsymbol{\theta}})\rho_{\boldsymbol{\theta}}\mathcal{R}_{\rho_{\boldsymbol{\theta}}}^{-1}(\partial_{\theta_\nu}\rho_{\boldsymbol{\theta}})\right] \\
&= \mathrm{Tr}\left[\sum_{i,j}\frac{2}{\lambda_i+\lambda_j}D^\mu_{ij}\left|\mathcal{G}'_i\right\rangle\!\left\langle\mathcal{G}'_j\right| \cdot \sum_{k\in\mathrm{supp}}\lambda_k\left|\mathcal{G}'_k\right\rangle\!\left\langle\mathcal{G}'_k\right| \cdot \sum_{m,n}\frac{2}{\lambda_m+\lambda_n}D^\nu_{mn}\left|\mathcal{G}'_m\right\rangle\!\left\langle\mathcal{G}'_n\right|\right] \\
&= \mathrm{Tr}\left[\sum_{i,j,m,n}\frac{2D^\mu_{ij}}{\lambda_i+\lambda_j}\cdot\frac{2D^\nu_{mn}}{\lambda_m+\lambda_n}\sum_{k\in\mathrm{supp}}\lambda_k\left|\mathcal{G}'_i\right\rangle\left\langle\mathcal{G}'_j|\mathcal{G}'_k\right\rangle\left\langle\mathcal{G}'_k|\mathcal{G}'_m\right\rangle\left\langle\mathcal{G}'_n\right|\right] \\
&= \mathrm{Tr}\left[\sum_{\substack{i,n\\k\in\mathrm{supp}}}\frac{2D^\mu_{ik}}{\lambda_i+\lambda_k}\cdot\frac{2D^\nu_{kn}}{\lambda_k+\lambda_n}\lambda_k\left|\mathcal{G}'_i\right\rangle\left\langle\mathcal{G}'_n\right|\right] \\
&= \sum_{\substack{n\in\mathrm{supp}\\k\in\mathrm{supp}}}\frac{2D^\mu_{nk}}{\lambda_n+\lambda_k}\cdot\frac{2D^\nu_{kn}}{\lambda_k+\lambda_n}\lambda_k + \sum_{\substack{n\in\mathrm{null}\\k\in\mathrm{supp}}}\frac{2D^\mu_{nk}}{\lambda_n+\lambda_k}\cdot\frac{2D^\nu_{kn}}{\lambda_k+\lambda_n}\lambda_k \\
&= \sum_{\substack{n\in\mathrm{supp}\\k\in\mathrm{supp}}}\frac{2D^\mu_{nk}D^\nu_{kn}}{\lambda_n+\lambda_k}\cdot\left(\frac{\lambda_k}{\lambda_k+\lambda_n}+\frac{\lambda_n}{\lambda_n+\lambda_k}\right) + \sum_{\substack{n\in\mathrm{null}\\k\in\mathrm{supp}}}\frac{2D^\mu_{nk}}{\lambda_k}\cdot\frac{2D^\nu_{kn}}{\lambda_k}\lambda_k \\
&= \sum_{\substack{n\in\mathrm{supp}\\k\in\mathrm{supp}}}\frac{2D^\mu_{nk}D^\nu_{kn}}{\lambda_n+\lambda_k} + \sum_{\substack{n\in\mathrm{null}\\k\in\mathrm{supp}}}\frac{4D^\mu_{nk}D^\nu_{kn}}{\lambda_k} \\
&= \sum_{\substack{n\in\mathrm{supp}\\k\in\mathrm{supp}}}2\frac{(\lambda_n-\lambda_k)^2}{\lambda_n+\lambda_k}\left\langle\partial_{\theta_\mu}\mathcal{G}'_n|\mathcal{G}'_k\right\rangle\left\langle\mathcal{G}'_k|\partial_{\theta_\nu}\mathcal{G}'_n\right\rangle + \sum_{\substack{n\in\mathrm{null}\\k\in\mathrm{supp}}}4\lambda_k\left\langle\mathcal{G}'_n|\partial_{\theta_\mu}\mathcal{G}'_k\right\rangle\left\langle\partial_{\theta_\nu}\mathcal{G}'_k|\mathcal{G}'_n\right\rangle \\
&= \sum_{\substack{n\in\mathrm{supp}\\k\in\mathrm{supp}}}2\frac{(\lambda_n-\lambda_k)^2}{\lambda_n+\lambda_k}\mathrm{Re}\left\{\left\langle\mathcal{G}_n|\boldsymbol{G}_\mu|\mathcal{G}_k\right\rangle\left\langle\mathcal{G}_k|\boldsymbol{G}_\nu|\mathcal{G}_n\right\rangle\right\} + \sum_{\substack{n\in\mathrm{null}\\k\in\mathrm{supp}}}4\lambda_k\mathrm{Re}\left\{\left\langle\mathcal{G}_k|\boldsymbol{G}_\mu|\mathcal{G}_n\right\rangle\left\langle\mathcal{G}_n|\boldsymbol{G}_\nu|\mathcal{G}_k\right\rangle\right\}.
\end{aligned}
\tag{90}
$$

Let us retrieve the pure state equation from this. Assume the quantum state density matrix can be described by that of a pure state $\rho = |\psi\rangle\langle\psi|$. This means $\lambda_1 = 1$ and every other $\lambda_j = 0$. Moreover, since independent of the $|\psi\rangle$ choice, one can always find an orthonormal basis such that $|\psi\rangle$ is part of. This means in particular that $\exists\mathcal{B} = \{|\psi_j\rangle\}_{j=1,\cdots,2^n}$, such that $|\psi_1\rangle = |\psi\rangle$ and $\sum_{j=1}^{2^n}|\psi_j\rangle\langle\psi_j| = \mathbb{1}$. Plugging ρ into Eq. 36 we get:

$$
\begin{aligned}
\mathcal{Q}_{\mu\nu}(\rho_{\boldsymbol{\theta}}) &= 4\mathrm{Re}\left\{\left\langle\psi_1\right|\boldsymbol{G}_\mu\left(\sum_{k=2}^{2^n}|\psi_k\rangle\langle\psi_k|\right)\boldsymbol{G}_\nu\left|\psi_1\right\rangle\right\} \\
&= 4\mathrm{Re}\left\{\left\langle\psi_1\right|\boldsymbol{G}_\mu\left(\mathbb{1}-|\psi_1\rangle\langle\psi_1|\right)\boldsymbol{G}_\nu\left|\psi_1\right\rangle\right\} \\
&= 4\mathrm{Re}\left\{\left\langle\psi_1\right|\boldsymbol{G}_\mu\boldsymbol{G}_\nu\left|\psi_1\right\rangle - \left\langle\psi_1\right|\boldsymbol{G}_\mu\left|\psi_1\right\rangle\left\langle\psi_1\right|\boldsymbol{G}_\nu\left|\psi_1\right\rangle\right\}.
\end{aligned}
\tag{91}
$$

This allows us to get one additional way to calculate the QFI of a mixed state. Suppose the density matrix is a sum of orthogonal states (even if it is not, there is always a decomposition into orthogonal states by changing basis, consequence of a diagonalization of the matrix). Let:

$$
\rho = \sum_{j\in\mathrm{supp}}\lambda_j\left|\mathcal{G}_j\right\rangle\!\left\langle\mathcal{G}_j\right|, \quad \text{such that } \left\langle\mathcal{G}_j|\mathcal{G}_k\right\rangle = \delta_{jk}.
\tag{92}
$$

Then:

$$
\begin{aligned}
\mathcal{Q}_{\mu\nu}(\rho_{\boldsymbol{\theta}}) &= \sum_{\substack{n\in\text{supp}\\k\in\text{supp}}} 2\frac{(\lambda_n-\lambda_k)^2}{\lambda_n+\lambda_k}\text{Re}\left\{\langle\mathcal{G}_n|\boldsymbol{G}_\mu|\mathcal{G}_k\rangle\langle\mathcal{G}_k|\boldsymbol{G}_\nu|\mathcal{G}_n\rangle\right\} + \sum_{\substack{n\in\text{null}\\k\in\text{supp}}} 4\lambda_k\text{Re}\left\{\langle\mathcal{G}_k|\boldsymbol{G}_\mu|\mathcal{G}_n\rangle\langle\mathcal{G}_n|\boldsymbol{G}_\nu|\mathcal{G}_k\rangle\right\}\\
&= \sum_{\substack{n\in\text{supp}\\k\in\text{supp}}} 2\frac{(\lambda_n-\lambda_k)^2}{\lambda_n+\lambda_k}\text{Re}\left\{a^\mu_{kn}a^\nu_{nk}\right\} + \sum_{k\in\text{supp}} 4\lambda_k\text{Re}\left\{\langle\mathcal{G}_k|\boldsymbol{G}_\nu\left[\sum_{n\in\text{null}}|\mathcal{G}_n\rangle\langle\mathcal{G}_n|\right]\boldsymbol{G}_\mu|\mathcal{G}_k\rangle\right\}\\
&= \sum_{\substack{n\in\text{supp}\\k\in\text{supp}}} 2\frac{(\lambda_n-\lambda_k)^2}{\lambda_n+\lambda_k}\text{Re}\left\{a^\mu_{kn}a^\nu_{nk}\right\} + \sum_{k\in\text{supp}} 4\lambda_k\text{Re}\left\{\langle\mathcal{G}_k|\boldsymbol{G}_\nu\left[\mathbb{1}-\sum_{n\in\text{supp}}|\mathcal{G}_n\rangle\langle\mathcal{G}_n|\right]\boldsymbol{G}_\mu|\mathcal{G}_k\rangle\right\}\\
&= \sum_{\substack{n\in\text{supp}\\k\in\text{supp}}} 2\frac{(\lambda_n-\lambda_k)^2}{\lambda_n+\lambda_k}\text{Re}\left\{a^\mu_{kn}a^\nu_{nk}\right\} + \sum_{k\in\text{supp}} 4\lambda_k\text{Re}\left\{\langle\mathcal{G}_k|\boldsymbol{G}_\nu\left[\mathbb{1}-|\mathcal{G}_k\rangle\langle\mathcal{G}_k|-\sum_{\substack{n\in\text{supp}\\n\neq k}}|\mathcal{G}_n\rangle\langle\mathcal{G}_n|\right]\boldsymbol{G}_\mu|\mathcal{G}_k\rangle\right\}\\
&= \sum_{\substack{n\in\text{supp}\\k\in\text{supp}}} 2\frac{(\lambda_n-\lambda_k)^2}{\lambda_n+\lambda_k}\text{Re}\left\{a^\mu_{kn}a^\nu_{nk}\right\} + \sum_{k\in\text{supp}}\lambda_k\mathcal{Q}_{\mu\nu}(|\mathcal{G}_k\rangle) - \sum_{\substack{n,k\in\text{supp}\\k\neq n}} 4\lambda_k\text{Re}\left\{a^\mu_{kn}a^\nu_{nk}\right\}\\
&= \sum_{\substack{n,k\in\text{supp}\\n\neq k}}\left[2\frac{(\lambda_n-\lambda_k)^2}{\lambda_n+\lambda_k}-4\lambda_k\right]\text{Re}\left\{a^\mu_{kn}a^\nu_{nk}\right\} + \sum_{k\in\text{supp}}\lambda_k\mathcal{Q}_{\mu\nu}(|\mathcal{G}_k\rangle)\\
&= \sum_{n>k\in\text{supp}} 4\left[\frac{(\lambda_n-\lambda_k)^2}{\lambda_n+\lambda_k}-(\lambda_n+\lambda_k)\right]\text{Re}\left\{a^\nu_{nk}a^\mu_{kn}\right\} + \sum_{k\in\text{supp}}\lambda_k\mathcal{Q}_{\mu\nu}(|\mathcal{G}_k\rangle).
\end{aligned}
\tag{93}
$$

In the case the state density matrix is described by a sum of non-orthogonal vectors:

$$
\rho = \sum_{j\in\text{supp}}\lambda_j|\phi_j\rangle\langle\phi_j|, \quad \text{such that } \langle\phi_j|\phi_k\rangle = \alpha_{jk}\leq 1, \tag{94}
$$

such that $\boldsymbol{G}_\mu|\phi_j\rangle$ is equal for every $|\phi_j\rangle$, then diagonalizing ρ into vectors that are orthogonal between themselves, call it $|\tilde{\phi}_j\rangle$ still holds the fact that $\boldsymbol{G}_\mu|\tilde{\phi}_j\rangle$ is equal for every $|\tilde{\phi}_j\rangle$. If, more than that, $\text{Re}\left\{a^\nu_{nk}a^\mu_{kn}\right\}\propto\mathcal{Q}_{\nu\mu}(|\mathcal{G}_n\rangle)$, then λ_n should simply be scaled into a $\tilde{\lambda}_n$, but the information is still structurally the same, *i.e.* it is the same function of parameters.

This gives some intuition about how to analyze Eq. 93 and when to use it over Eq. 90. In Eq. 93 the first term corresponds to a distinguishability between the states under the encoding dynamics. If the generators of the dynamics are orthogonal to the noise, then this goes to zero. The second part of Eq. 93 can be seen as the local informations of each states in a perfect scenario weighted by the corresponding weights. Note that the expression:

$$
4\left[\frac{(\lambda_n-\lambda_k)^2}{\lambda_n+\lambda_k}-(\lambda_n+\lambda_k)\right],
$$

is always negative, meaning that if they are completely distinguishable, then we recover the notion of convexity of the QFI. If they are not completely distinguishable, then the amount of information is decreased by a factor proportional to $\text{Re}\left\{a^\nu_{nk}a^\mu_{kn}\right\}$. On the other hand, when the noise is only in the same direction of the generators of the encoding, then Eq. 90 becomes simpler, as the second part goes to zero, and we are left simply with an expression that weights the distinguishability of the states, under the encoding dynamics.