

Privacy in Continuous-Variable Distributed Quantum Sensing

A. de Oliveira Junior^{1,*}, Anton L. Andersen², Benjamin Lundgren Larsen,¹ Sean William Moore,² Damian Markham², Masahiro Takeoka^{3,4}, Jonatan Bohr Brask¹, and Ulrik L. Andersen¹

¹*Center for Macroscopic Quantum States bigQ, Department of Physics, Technical University of Denmark, Fysikvej 307, 2800 Kgs. Lyngby, Denmark*

²*Sorbonne Université, CNRS, LIP6, F-75005 Paris, France*

³*Department of Electronics and Electrical Engineering, Keio University, 3-14-1 Hiyoshi, Kohoku-ku, Yokohama 223-8522, Japan*

⁴*Advanced ICT Research Institute, National Institute of Information and Communications Technology (NICT), Koganei, Tokyo 184-8795, Japan*



(Received 25 September 2025; accepted 27 July 2026; published 21 August 2026)

Can a distributed network of quantum sensors estimate a global parameter while protecting every locally encoded value? We answer this question affirmatively by introducing and analyzing a protocol for distributed quantum sensing in the continuous-variable regime. We consider a multipartite network in which an unknown local phase is imprinted at each node on a shared entangled Gaussian state. We show that the average phase can be estimated with high precision, exhibiting Heisenberg scaling in the total photon number, while individual phases are inaccessible. We further prove a no-go theorem showing that, for three or more parties, no finite-energy Gaussian probe can provide complete privacy of the average phase, meaning that all phase combinations orthogonal to the average remain entirely hidden. This identifies the two-party case as an exceptional Gaussian setting that can achieve complete privacy. We further investigate the impact of displacements and optical losses, revealing trade-offs between estimation accuracy and privacy. Finally, we benchmark the protocol against other continuous-variable resource states.

DOI: [10.1103/1psz-clqx](https://doi.org/10.1103/1psz-clqx)

I. INTRODUCTION

Sensing spatially distributed parameters lies at the heart of emerging quantum technologies, with implications ranging from clock synchronization [1,2] to distributed computing [3,4] and precision metrology [5,6]. Over the past two decades, we have learned how quantum information may be processed, shared, and protected across networks [7–11]. Within this landscape, quantum sensor networks, in which entangled resources are distributed among spatially separated nodes that collaboratively estimate parameters, have emerged as powerful platforms for both fundamental studies and real-world applications [6,12–19].

A central challenge in any such network is privacy, meaning that each node should learn only the authorized global quantity while remaining ignorant of the individual

parameters. A paradigmatic example is distributed phase sensing, where each node encodes an unknown local phase and the network aims to estimate only the average phase, while keeping all individual phases and non-target phase combinations hidden [20,21]. In this setting, each local phase is an unknown physical parameter imprinted at a node by a local channel. The party operating that node follows the prescribed measurement procedure, but does not know the value of its phase except through the quantum probe and the public measurement record. Likewise, a party or external observer may access the full public classical record and any quantum systems assigned to them, but has no direct side information about the raw local phase values. Operationally, this setting captures applications ranging from networked atomic clocks, where the encoded phase represents a local clock offset and the target is an average synchronization signal [1,2], to distributed magnetic-field or strain sensing, where local fields are encoded as phases but only an aggregate quantity is revealed [13,16,19]. It also encompasses more general quantum sensor networks estimating linear functions of spatially distributed parameters [6,14,15,22], as well as quantum-assisted long-baseline interferometry, where separated sites jointly estimate optical phase information without each site accessing the full global signal [9,23,24].

*Contact author: alexssandreoliveira@gmail.com

Published by the American Physical Society under the terms of the [Creative Commons Attribution 4.0 International](https://creativecommons.org/licenses/by/4.0/) license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

While discrete-variable quantum networks have protocols for private parameter estimation [20,25,26], including experimental demonstrations [27], optimal state constructions [21], and analyses of robustness against noise and loss [28,29], the corresponding question for continuous-variable (CV) sensor networks remains largely unexplored. In particular, it is not known whether CV systems can achieve complete privacy, whether weaker forms of privacy are possible, or how these privacy requirements affect the precision with which the target function can be estimated. This gap is especially striking because optical Gaussian states provide deterministic, large-scale entanglement at room temperature [30,31]. This motivates the key question addressed in the present work: under an experimentally feasible protocol, can CV sensor networks be made private and, if so, what price must be paid in precision?

We answer this question by proving a no-go theorem showing that, for three or more parties, finite-energy Gaussian states cannot hide every phase combination orthogonal to the average phase, and therefore cannot provide complete privacy. The two-party case is the exceptional setting allowed by our result, where a two-mode squeezed state can achieve complete privacy. For larger networks, the attainable goal is instead privacy at the level of individual local phases. We then identify a simple, experimentally feasible Gaussian protocol, based on distributing a two-mode squeezed vacuum through a beam-splitter network, that preserves the privacy of every individual local phase and asymptotically approaches complete privacy (see Fig. 1 for a schematic representation). We also show that the average phase can be estimated with high precision, exhibiting Heisenberg

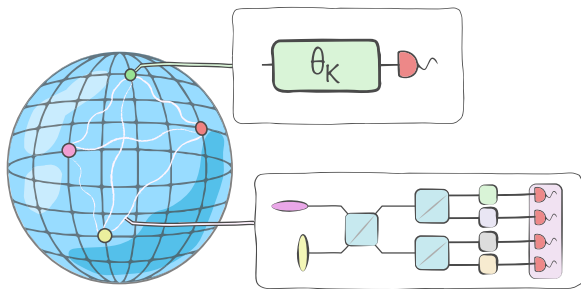


FIG. 1. Phase estimation & privacy. Two squeezed states are combined at a local beam splitter to generate a two-mode squeezed state, which is then split into four modes using two additional beam splitters. Each party receives one mode, and a local phase θ_k is encoded. The goal is to estimate the average phase while hiding the individual local phases. The strongest version would hide every combination orthogonal to the average (complete privacy). For Gaussian probes of three or more modes complete privacy is ruled out, so the multipartite protocol targets the privacy of each local phase (weak privacy) and quantifies residual leakage into other combinations.

scaling in the total photon number, while other orthogonal phase combinations exhibit shot-noise scaling. Our results reveal a fundamental limitation on the use of Gaussian resources for privacy in distributed quantum sensing. They also complement recent work [32] by resolving the open question of whether Gaussian states can achieve complete privacy.

The paper is organized as follows. In Sec. II, we introduce the estimation task, the notion of privacy, the quantum Fisher information matrix (QFIm)-based privacy criterion, and the Gaussian formalism used throughout. There, we also derive a general QFIm formula for pure Gaussian states under local phase encoding in Lemma 2, together with a covariance-matrix expression for the privacy measure in Theorem 3. In Sec. III, we first prove the no-go theorem for complete average-phase privacy with three or more Gaussian modes in Theorem 4. We then present the two-mode squeezed state as the exceptional two-party case achieving complete privacy, including the effects of finite squeezing and loss, before introducing the multipartite beam-splitter protocol. For this protocol, we characterize the QFIm in Lemma 5, derive its spectrum in Theorem 6, and analyze its privacy properties in Corollary 7. In Sec. IV, we study the effects of displacement and optical loss, and benchmark the protocol against other Gaussian resources, including independent single-mode squeezed states and cluster states. We conclude with a summary and outlook, while the appendices contain the technical proofs and supporting examples.

II. SETTING THE SCENE

This section sets out the estimation problem, the estimation-theoretic tools we use, the operational notions of privacy, and the Gaussian framework in which we work. We first introduce the multiparameter setting and the quantum Fisher information matrix, whose range and kernel determine which linear combinations of phases are locally estimable. We then define unobservable directions, private parameters, and the privacy regimes considered in the rest of the paper, together with the assumptions on the parties under which these guarantees apply. Finally, we specialize the formalism to Gaussian states and operations.

A. Multiparameter estimation problem

We consider a network of M parties, connected by quantum and classical links, that share an initial joint quantum state $\hat{\rho}$. Each party μ is subjected to a local encoding channel $\Lambda_\mu(\theta_\mu)$ that imprints an unknown parameter $\theta_\mu \in \mathbb{R}$ on its share [see Fig. 2(a)]. The resulting encoded state is $\hat{\rho}(\boldsymbol{\theta}) := \Lambda_{\boldsymbol{\theta}}(\hat{\rho})$, where $\Lambda_{\boldsymbol{\theta}} := \bigotimes_{\mu=1}^M \Lambda_\mu(\theta_\mu)$, with $\boldsymbol{\theta} = (\theta_1, \dots, \theta_M) \in \mathbb{R}^M$ [see Fig. 2(b)]. After encoding, every node performs a measurement and broadcasts its classical outcome to a trusted central processor [see

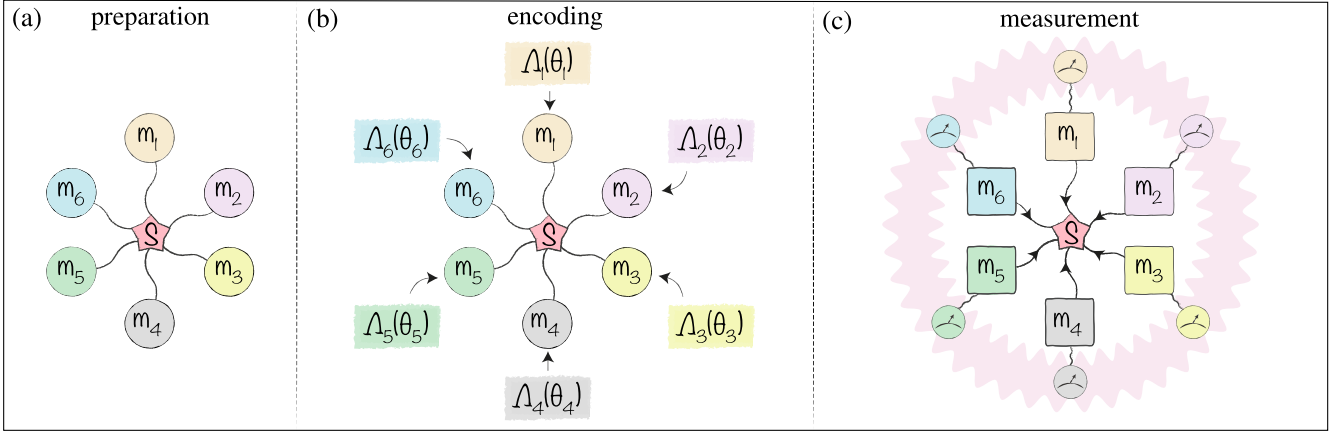


FIG. 2. Estimation scheme. The parties (depicted as colored circles) request an M -partite state ρ_0 from the source S (red star), which (a) prepares and distributes it within the network. Then, (b) an unknown parameter θ_μ is locally encoded via a quantum operation $\Lambda_\mu(\theta_\mu)$. After encoding, (c) the probe is measured either locally at the nodes, with the outcomes broadcast publicly, or by a joint receiver, and the resulting data are processed by a trusted central processor.

Fig. 2(c)]. The collective task is to estimate, from these broadcast outcomes, a publicly agreed linear target function $f(\theta) = \mathbf{u}^T \theta$ where $\mathbf{u} \in \mathbb{R}^M$ and $\|\mathbf{u}\|_2 = 1$.

The fundamental object that bounds the precision of any unbiased estimator of θ is the QFI, with entries [33–36]

$$\mathcal{Q}_{\mu\nu}[\hat{\rho}(\theta)] := \frac{1}{2} \text{tr}[\hat{\rho}(\theta) \{\hat{L}_{\theta_\mu}, \hat{L}_{\theta_\nu}\}], \quad (1)$$

where $\{\hat{A}, \hat{B}\} = \hat{A}\hat{B} + \hat{B}\hat{A}$ denotes the anticommutator and $2\partial_{\theta_\nu} \hat{\rho}(\theta) = \hat{\rho}(\theta) \hat{L}_{\theta_\nu} + \hat{L}_{\theta_\nu} \hat{\rho}(\theta)$ is the symmetric logarithmic derivative (SLD). The QFI $\mathcal{Q}$ is a real, symmetric, positive semi-definite matrix. Its spectrum governs the achievable estimation precision and, as we will see, also the information that can leak about θ . We will use two subspaces of $\mathbb{R}^M$:

$$\text{range}(\mathcal{Q}) := \{\mathcal{Q}\mathbf{u} : \mathbf{u} \in \mathbb{R}^M\} \subseteq \mathbb{R}^M, \quad (2)$$

i.e., the linear span of the columns of $\mathcal{Q}$. The *kernel* (or null space) is

$$\ker \mathcal{Q} := \{\mathbf{u} \in \mathbb{R}^M : \mathcal{Q}\mathbf{u} = \mathbf{0}\}, \quad (3)$$

equivalently, the subspace of vectors that $\mathcal{Q}$ maps to zero. For symmetric $\mathcal{Q}$, $\text{range}(\mathcal{Q})$ and $\ker \mathcal{Q}$ are orthogonal complements in $\mathbb{R}^M$.

A linear function $\mathbf{u}^T \theta$ admits a finite-variance, locally unbiased estimator if and only if $\mathbf{u} \in \text{range}(\mathcal{Q})$. When this holds, the scalar quantum Cramér-Rao bound is [37,38]

$$\text{var}(\mathbf{u}^T \hat{\theta}) \geq \mathbf{u}^T \mathcal{Q}^+ \mathbf{u}, \quad (4)$$

where $\mathcal{Q}^+$ is the Moore-Penrose pseudoinverse. The condition $\mathbf{u} \in \text{range}(\mathcal{Q})$ is essential. If $\mathbf{u}$ has a component along $\ker \mathcal{Q}$, then that component lies in an unobservable

direction. To make this explicit, decompose $\mathbf{u}$ orthogonally as $\mathbf{u} = \mathbf{u}_r + \mathbf{u}_0$, with $\mathbf{u}_r \in \text{range}(\mathcal{Q})$ and $\mathbf{u}_0 \in \ker \mathcal{Q}$. For $\epsilon > 0$, we regularize the QFI as $\mathcal{Q} + \epsilon \mathbb{1}$ and denote $\mathcal{Q}_r$ the restriction of $\mathcal{Q}$ to $\text{range}(\mathcal{Q})$. Since $\text{range}(\mathcal{Q})$ and $\ker \mathcal{Q}$ are orthogonal invariant subspaces of $\mathcal{Q}$, one obtains

$$\mathbf{u}^T (\mathcal{Q} + \epsilon \mathbb{1})^{-1} \mathbf{u} = \mathbf{u}_r^T (\mathcal{Q}_r + \epsilon \mathbb{1})^{-1} \mathbf{u}_r + \frac{\|\mathbf{u}_0\|_2^2}{\epsilon}, \quad (5)$$

which diverges as $\epsilon \rightarrow 0^+$ whenever $\mathbf{u}_0 \neq \mathbf{0}$. Any component of $\mathbf{u}$ in $\ker \mathcal{Q}$ is therefore *unobservable*. No locally unbiased estimator of the corresponding linear combination of θ can have finite variance. For the unitary encodings considered in this work an even stronger statement holds. As shown below, $\mathbf{u} \in \ker \mathcal{Q}$ implies the exact invariance $\hat{\rho}(\theta + t\mathbf{u}) = \hat{\rho}(\theta)$ for all $t \in \mathbb{R}$, so every measurement produces statistics that are strictly independent of the parameter combination along $\mathbf{u}$, and that combination is nonidentifiable rather than merely poorly estimable (see Definition 1 and Lemma 8 in Appendix A). We use $\mathcal{Q}^+$ in subsequent expressions only as shorthand on $\text{range}(\mathcal{Q})$, and we always identify a kernel direction explicitly as unobservable rather than as having vanishing variance. Thus, when $\mathbf{u} \notin \text{range}(\mathcal{Q})$, the finite number $\mathbf{u}^T \mathcal{Q}^+ \mathbf{u}$ is not interpreted as a precision bound for the full target $\mathbf{u}^T \theta$. These observations motivate the following definition.

Definition 1. (Unobservable direction & private parameter). Let $\mathcal{Q}(\theta)$ be the QFI of the encoded state $\hat{\rho}(\theta)$ and define the directional derivative

$$\partial_{\mathbf{u}} \hat{\rho}(\theta) := \sum_{\mu=1}^M u_\mu \partial_{\theta_\mu} \hat{\rho}(\theta). \quad (6)$$

1. A nonzero vector $\mathbf{u} \in \mathbb{R}^M$ is unobservable at θ if $\mathbf{u} \in \ker \mathcal{Q}(\theta)$.

2. A component θ_j is private at θ if there exists an unobservable $\mathbf{u}$ with $u_j \neq 0$.

Equivalently, θ_j is private if and only if $\mathbf{e}_j \notin \text{range}(\mathbf{Q})$, where $\mathbf{e}_j$ is the unit vector with a 1 in the j -th entry (see Proposition 1 below). We note that the definition of unobservability, $\mathbf{u} \in \ker \mathbf{Q}$, coincides with $\partial_{\mathbf{u}} \hat{\rho} = 0$ at regular points (see Lemma 8 in Appendix A), where $\hat{\rho}(\theta)$ has locally constant rank and depends smoothly on θ [35,39]. Outside such points, parameter-dependent changes in the rank of $\hat{\rho}$ can produce singular Fisher-information contributions through the limiting behavior of $\frac{(\partial_{\mathbf{u}} p_k)^2}{p_k}$, where $p_k(\theta)$ is an eigenvalue of $\hat{\rho}$ satisfying $p_k(\theta_0) = \partial_{\mathbf{u}} p_k(\theta_0) = 0$ at an interior point θ_0 [40,41]. Although both the numerator and denominator vanish at θ_0 , the limiting ratio along $\mathbf{u}$ can be finite and nonzero. In the protocols studied here the parameter dependence is purely unitary, so the spectrum of $\hat{\rho}(\theta)$ is independent of θ and $\frac{\partial p_k}{\partial \theta} \equiv 0$ for every eigenvalue (including zero eigenvalues). The rank of $\hat{\rho}(\theta)$ is locally constant, and no singular eigenvalue contribution arises. The only non-unitary channel we model—a fixed loss before the phase encoding—is itself θ -independent and so does not introduce parameter-dependent support either. The regular-point equivalence between $\mathbf{u} \in \ker \mathbf{Q}$ and $\partial_{\mathbf{u}} \hat{\rho} = 0$ therefore holds throughout this work.

We conclude this section with a proposition that characterizes private parameters:

Proposition 1. (Characterization of private parameters). For a real symmetric QFI $\mathbf{Q}$, a component θ_j is private at θ if and only if $\mathbf{e}_j \notin \text{range}(\mathbf{Q})$. Equivalently, θ_j is private if and only if there exists $\mathbf{u} \in \ker \mathbf{Q}$ with $u_j \neq 0$.

Proof. Because $\mathbf{Q}$ is real and symmetric, $\text{range}(\mathbf{Q}) = (\ker \mathbf{Q})^\perp$. If there exists $\mathbf{u} \in \ker \mathbf{Q}$ with $u_j \neq 0$, then $\mathbf{e}_j^\top \mathbf{u} = u_j \neq 0$, so $\mathbf{e}_j$ is not orthogonal to $\ker \mathbf{Q}$ and therefore cannot belong to $\text{range}(\mathbf{Q})$. Conversely, if $\mathbf{e}_j \notin \text{range}(\mathbf{Q})$, then its orthogonal projection $\mathbf{u}$ onto $\ker \mathbf{Q}$ is nonzero. Since $\mathbf{e}_j - \mathbf{u} \in \text{range}(\mathbf{Q})$ and $\mathbf{u} \in \ker \mathbf{Q}$, these two vectors are orthogonal. Hence $0 = \mathbf{u}^\top (\mathbf{e}_j - \mathbf{u}) = u_j - \|\mathbf{u}\|_2^2$, so $u_j = \|\mathbf{u}\|_2^2 > 0$. Thus $\mathbf{u} \in \ker \mathbf{Q}$ and $u_j \neq 0$. By Definition 1, this is exactly the condition that θ_j is private. ■

B. Privacy characterization and quantification

We can now state the operational notions of privacy that organize the rest of the paper, together with the assumptions on the parties under which our results hold. Each party holds one mode of an entangled probe distributed by a trusted source. The parameter θ_μ is an unknown physical phase imprinted on mode μ by the local environment—a sample, an external field, a refractive-index shift, a clock offset, or another local channel. Each party operates the post-encoding readout apparatus at its node and follows the prescribed measurement procedure, but does not know

the numerical value of θ_μ except through the quantum probe and the public measurement record. The privacy task is to ensure that no party, colluding subset of parties, or external observer with access to the public broadcast and to the quantum systems in their possession can uniquely reconstruct any raw individual value, except insofar as it is unavoidably constrained by the authorized target function.

We work under the following prescribed-protocol assumptions:

A₁. Trusted source. A trusted source prepares the requested probe within a known tolerance and distributes it through the network. The only state imperfection we model is optical loss in the distribution channels.

A₂. Access-controlled & no-side-information. The parameter θ_μ is an unknown external physical quantity imprinted once on the designated mode during a prescribed sensing interaction at node μ . Party μ operates the post-encoding readout, but is neither given θ_μ nor able to substitute an auxiliary probe or obtain an additional use of the parameter-dependent interaction.

A₃. Prescribed-protocol execution. The parties perform the agreed measurement and report its outcome truthfully.

A₄. Available information. A party, a colluding subset of nodes, or an external observer may have access to (i) the entire public classical record, namely all broadcast measurement outcomes, and (ii) the quantum systems in their possession. They do not have direct access to any raw local parameter value θ_ν , including the value encoded at their own node, except through the quantum systems in their possession and the public classical record.

The privacy guarantees below are information-theoretic statements about the impossibility of uniquely inferring the protected parameter values from the accessible information. The restriction in **A₂** is a physical access assumption, not a property enforced by the shared probe. If a party could substitute an auxiliary probe or repeat the parameter-dependent interaction, no shared state could prevent it from estimating θ_μ directly. Assumption **A₃** concerns only the stated estimation performance and the integrity of the reported estimate. For privacy, the parties may process arbitrarily the quantum systems in their possession and the public record, as specified in **A₄**. The privacy guarantee does not cover additional access to the sensing interaction contrary to **A₂** or direct side information about the raw parameters and is not a composable cryptographic guarantee. The only integrity-relevant imperfection we model is optical loss in the distribution channels. Relaxing these conditions using verification protocols for untrusted sources [25,42] is discussed in the conclusions.

Here and throughout, $\mathbf{Q}$ denotes the QFI of the full encoded state, without imposing an LOCC restriction on

the measurement. Conclusions concerning complete and component privacy that are derived from $\ker \mathbf{Q}$ are measurement independent: for the unitary phase encodings considered here, a kernel direction leaves the encoded state invariant and is therefore unobservable under any POVM. By contrast, Eq. (4) and the nonzero eigenvalues of $\mathbf{Q}$ provide unrestricted-measurement precision benchmarks. Their attainability by local measurements is not assumed for general M .

We now organize privacy in terms of the range and kernel of the QFI. Fix a target direction $\mathbf{u} \in \mathbb{R}^M$ with $\|\mathbf{u}\|_2 = 1$. We exclude the operationally degenerate single-component case $\mathbf{u} = \pm \mathbf{e}_j$, since asking the protocol to reveal θ_j while simultaneously keeping it private is inconsistent. Complete privacy is the strongest case, in which only the target function $f(\boldsymbol{\theta}) = \mathbf{u}^\top \boldsymbol{\theta}$ is accessible. A weaker requirement is component privacy, where every individual phase remains private even though some non-target linear combinations may still be accessible. For non-coordinate targets, complete privacy implies component privacy, but the converse need not hold.

To obtain a quantitative measure, rather than only a binary distinction between private and non-private directions, we use the measure of Ref. [28]:

$$P(\mathbf{Q}, \mathbf{u}) = \frac{\mathbf{u}^\top \mathbf{Q} \mathbf{u}}{\text{tr}(\mathbf{Q})}. \quad (7)$$

The privacy measure is evaluated with $\|\mathbf{u}\|_2 = 1$, so that $0 \leq P(\mathbf{Q}, \mathbf{u}) \leq 1$ whenever $\mathbf{Q} \neq \mathbf{0}$. It is undefined when $\text{tr} \mathbf{Q} = 0$, which corresponds to the encoded state being locally invariant under all single-parameter shifts. Moreover, $P(\mathbf{Q}, \mathbf{u}) = 1$ if and only if $\mathbf{Q}$ is rank one and $\text{range}(\mathbf{Q}) = \text{span}\{\mathbf{u}\}$, equivalently $\mathbf{Q} \propto \mathbf{u} \mathbf{u}^\top$. The measure has two convenient properties: it is basis invariant, $P(\mathbf{B} \mathbf{Q} \mathbf{B}^\top, \mathbf{B} \mathbf{u}) = P(\mathbf{Q}, \mathbf{u})$ for any real orthogonal matrix $\mathbf{B}$, and it is continuous in $\mathbf{Q}$, so small experimental imperfections lead to proportionally small changes in P . Finally, $P(\mathbf{Q}, \mathbf{u}) > 0$ does not by itself imply that the target $f(\boldsymbol{\theta})$ is estimable. This can happen because $\mathbf{u}$ may have a component in $\ker \mathbf{Q}$, which does not contribute to $\mathbf{u}^\top \mathbf{Q} \mathbf{u}$ but nevertheless prevents $\mathbf{u}^\top \hat{\boldsymbol{\theta}}$ from having finite variance.

The scalar quantity $P(\mathbf{Q}, \mathbf{u})$ is useful for quantifying how concentrated the Fisher information is along the target direction, but it does not by itself determine which individual parameters are private. We therefore keep track of the kernel and range of $\mathbf{Q}$ explicitly. In the following classification, we assume $\mathbf{Q} \geq 0$, $\text{tr} \mathbf{Q} > 0$, a non-degenerate target $\mathbf{u} \neq \pm \mathbf{e}_j$, and local estimability of the target, $\mathbf{u} \in \text{range}(\mathbf{Q})$. Cases with $\mathbf{u} \notin \text{range}(\mathbf{Q})$ are excluded, since then the target itself is unobservable. Under these assumptions, the regimes below distinguish complete privacy, weak component privacy, partial hiding, and the absence of component privacy.

1. *Complete privacy* ($\text{range}(\mathbf{Q}) = \text{span}\{\mathbf{u}\}$, equivalently $P = 1$ and $\dim \ker \mathbf{Q} = M - 1$): only $f(\boldsymbol{\theta})$ is accessible.
2. *Weak component privacy* ($\mathbf{e}_j \notin \text{range}(\mathbf{Q})$ for every j , but $\text{range}(\mathbf{Q}) \supsetneq \text{span}\{\mathbf{u}\}$): every individual component is private, but some non-target combinations remain accessible.
3. *Partial hiding* ($\dim \ker \mathbf{Q} \geq 1$, but $\mathbf{e}_j \in \text{range}(\mathbf{Q})$ for at least one j): some linear combinations are unobservable, but at least one individual component θ_j is accessible.
4. *No component privacy* ($\ker \mathbf{Q} = \{\mathbf{0}\}$): every component θ_j is observable.

The following box illustrates these notions on a few discrete-variable warm-ups; analogous Gaussian examples are worked out in Sec. III.

Example: privacy measure for GHZ, W & $|+\rangle^{\otimes 3}$

As a warm-up, consider three parties sharing a given state $|\psi\rangle$. Each party j locally encodes a phase θ_j by applying the unitary operation $U(\theta_j) = |0\rangle\langle 0| + e^{i\theta_j}|1\rangle\langle 1|$. The aim is to estimate the average phase, characterized by a vector $\mathbf{v}_{\text{avg}} \propto (1, 1, 1)$, while remaining completely agnostic about other combinations of the individual phases. The privacy measure for different choices of the initial state (see Appendix B for details) is given by

$$(a) \quad |\text{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \rightarrow P(\mathbf{Q}_{\text{GHZ}}, \mathbf{v}_{\text{avg}}) = 1.$$

Here $\mathbf{Q}_{\text{GHZ}}$ is the all-ones matrix. Its kernel is the two-dimensional subspace $\{\mathbf{u}: u_1 + u_2 + u_3 = 0\}$, so for each j there exist null vectors with $u_j \neq 0$. Hence every individual phase θ_j is private. The only observable combination is the sum $\theta_1 + \theta_2 + \theta_3$, which coincides with the chosen target.

$$(b) \quad |\text{W}\rangle = \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle) \rightarrow P(\mathbf{Q}_{\text{W}}, \mathbf{v}_{\text{avg}}) = 0.$$

One has $\ker \mathbf{Q}_{\text{W}} = \text{span}\{(1, 1, 1)\}$ (any global shift of all three phases is invisible), so $\mathbf{Q}_{\text{W}}$ has rank two. Because the null vector has all three nonzero components, each θ_j is private. However, the average-phase direction lies entirely in the kernel, so $\mathbf{v}_{\text{avg}} \notin \text{range}(\mathbf{Q}_{\text{W}})$ and the average phase is unobservable. The W state is therefore target-blind for the average. The privacy measure registers this as $P(\mathbf{Q}_{\text{W}}, \mathbf{v}_{\text{avg}}) = 0$.

$$(c) \quad |+\rangle^{\otimes 3} = \left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right]^{\otimes 3} \rightarrow P(\mathbf{Q}_{+}, \mathbf{v}_{\text{avg}}) = \frac{1}{3}.$$

In this case, $\mathbf{Q}_{+}$ is full rank (no kernel), so there is no null direction with $u_j \neq 0$. By Definition 1 no individual phase is private. The probe reveals all three phases (and thus the average), with $P(\mathbf{Q}_{+}, \mathbf{v}_{\text{avg}}) = \frac{1}{3}$ indicating that only one third of the total information is aligned with the average and the rest leaks into orthogonal combinations.

C. Gaussian framework

We now restrict the framework above to Gaussian states and operations, which form the resource class used in the rest of the paper.

We consider quantum systems with M canonical degrees of freedom, with annihilation and creation operators $\hat{a}_\mu$ and $\hat{a}_\mu^\dagger$ ($\mu \in \{1, \dots, M\}$). Setting $\hbar = 1$, the canonical commutation relations are $[\hat{a}_\mu, \hat{a}_\nu] = [\hat{a}_\mu^\dagger, \hat{a}_\nu^\dagger] = 0$ and $[\hat{a}_\mu, \hat{a}_\nu^\dagger] = \delta_{\mu\nu}$. Hermitian quadratures are defined by $\hat{x}_\mu = \frac{1}{\sqrt{2}}(\hat{a}_\mu + \hat{a}_\mu^\dagger)$ and $\hat{p}_\mu = \frac{1}{i\sqrt{2}}(\hat{a}_\mu - \hat{a}_\mu^\dagger)$, satisfying $[\hat{x}_\mu, \hat{p}_\nu] = i\delta_{\mu\nu}$. Collecting them in the column vector $\hat{\mathbf{r}} = (\hat{x}_1, \hat{p}_1, \dots, \hat{x}_M, \hat{p}_M)^\top$, one has $[\hat{\mathbf{r}}, \hat{\mathbf{r}}^\top] = i\Omega$, where Ω is the symplectic form. Throughout, $M \in \mathbb{N}$ denotes the number of bosonic modes (and the number of users); the auxiliary symbol $N \in \mathbb{N}$ appears only in recursive constructions, e.g. $M = 2^N$.

A Gaussian state is completely characterized by its first moments and covariance matrix [43–45],

$$\bar{\mathbf{r}} = \text{tr}(\hat{\rho} \hat{\mathbf{r}}) \quad \text{and} \quad \boldsymbol{\sigma} = \frac{1}{2} \text{tr}[\hat{\rho}\{(\hat{\mathbf{r}} - \bar{\mathbf{r}}), (\hat{\mathbf{r}} - \bar{\mathbf{r}})^\top\}]. \quad (8)$$

Gaussian operations act on $(\boldsymbol{\sigma}, \bar{\mathbf{r}})$ via $\boldsymbol{\sigma} \rightarrow \mathbf{F}\boldsymbol{\sigma}\mathbf{F}^\top$, $\bar{\mathbf{r}} \rightarrow \mathbf{F}\bar{\mathbf{r}} + \mathbf{d}$ with $\mathbf{F}\Omega\mathbf{F}^\top = \Omega$. For pure Gaussian states, the QFI can be written as [46]

$$\mathcal{Q}_{\mu\nu}(\boldsymbol{\sigma}, \bar{\mathbf{r}}) = \frac{1}{4} \text{tr}[(\boldsymbol{\sigma}^{-1} \partial_{\theta_\mu} \boldsymbol{\sigma})(\boldsymbol{\sigma}^{-1} \partial_{\theta_\nu} \boldsymbol{\sigma})] + \partial_{\theta_\mu} \bar{\mathbf{r}}^\top \boldsymbol{\sigma}^{-1} \partial_{\theta_\nu} \bar{\mathbf{r}}. \quad (9)$$

The inverse $\boldsymbol{\sigma}^{-1}$ here refers to the covariance matrix only. Every physical Gaussian state satisfies $\boldsymbol{\sigma} \succ 0$, so $\boldsymbol{\sigma}^{-1}$ is always well defined. This should not be confused with full rank of the density operator, which fails for pure Gaussian states. The first term in Eq. (9) encodes the information stored in the covariances, while the second accounts for the displacements; either term vanishes when the corresponding quantity is parameter-independent.

In the Gaussian protocols studied below, the local parameters are encoded as phase shifts generated by the number operators $\hat{n}_\mu = \hat{a}_\mu^\dagger \hat{a}_\mu$. The encoded family is

$$\hat{\rho}(\boldsymbol{\theta}) = \hat{U}(\boldsymbol{\theta}) \hat{\rho} \hat{U}(\boldsymbol{\theta})^\dagger \quad \text{where} \quad \hat{U}(\boldsymbol{\theta}) = \bigotimes_{\mu=1}^M e^{i\theta_\mu \hat{n}_\mu}. \quad (10)$$

For a generic pure multimode Gaussian state subjected to the local phase encoding in Eq. (10), the quantum Fisher information matrix can be expressed directly in terms of the covariance matrix and first moments. The following result gives the corresponding closed-form expression:

Lemma 2. (QFI for Gaussian phase shifts). Let $|\Psi(\boldsymbol{\theta})\rangle$ be a pure M -mode Gaussian state obtained by applying

local phase shifts to a pure state $|\psi_0\rangle$

$$|\Psi(\boldsymbol{\theta})\rangle = \left(\bigotimes_{\mu=1}^M e^{i\theta_\mu \hat{n}_\mu} \right) |\psi_0\rangle, \quad (11)$$

The quantum Fisher information matrix associated with multiparameter phase estimation $\boldsymbol{\theta} = (\theta_1, \dots, \theta_M)$ can be expressed in terms of the quadrature covariance matrix and first moments as follows:

$$\mathcal{Q}_{\mu\nu} = 2 \sum_{z,w \in \{x,p\}} (\sigma_{\hat{z}_\mu \hat{w}_\nu}^2 + 2 \sigma_{\hat{z}_\mu \hat{w}_\nu} \bar{\mathbf{r}}_{\hat{z}_\mu} \bar{\mathbf{r}}_{\hat{w}_\nu}) - \delta_{\mu\nu}. \quad (12)$$

where $\sigma_{\hat{z}_\alpha \hat{w}_\beta} := \langle (\hat{z}_\alpha - \bar{\mathbf{r}}_{\hat{z}_\alpha})(\hat{w}_\beta - \bar{\mathbf{r}}_{\hat{w}_\beta}) \rangle$ denotes the centered second moment and $\bar{\mathbf{r}}_{\hat{z}_\alpha} = \langle \hat{z}_\alpha \rangle$.

The proof of the above lemma is given in Appendix E. Lemma 2 also enables us to derive the following theorem for the privacy measure:

Theorem 3. (Privacy in Gaussian phase estimation). The privacy when estimating the average phase from a pure M -mode Gaussian state $|\Psi(\boldsymbol{\theta})\rangle$, where each local parameter θ_μ is encoded via $U_\mu(\theta_\mu) = e^{i\theta_\mu \hat{n}_\mu}$, is given by

$$P(\mathcal{Q}, \mathbf{v}_{\text{avg}}) = \frac{2 \sum_{z,w \in \{x,p\}}^{\mu,\nu} (\sigma_{\hat{z}_\mu \hat{w}_\nu}^2 + 2 \sigma_{\hat{z}_\mu \hat{w}_\nu} \bar{\mathbf{r}}_{\hat{z}_\mu} \bar{\mathbf{r}}_{\hat{w}_\nu}) - M}{M (2 \sum_{z,w \in \{x,p\}}^{\mu} (\sigma_{\hat{z}_\mu \hat{w}_\mu}^2 + 2 \sigma_{\hat{z}_\mu \hat{w}_\mu} \bar{\mathbf{r}}_{\hat{z}_\mu} \bar{\mathbf{r}}_{\hat{w}_\mu}) - M)}, \quad (13)$$

where the above summation denotes the double sum over μ, ν and $z, w \in \{x, p\}$.

The proof is in Appendix E.

III. MAIN RESULTS

The framework of Sec. II reduces the privacy of a distributed phase-sensing protocol to a property of the QFI. We now take the target direction to be the average-phase direction, $\mathbf{u} = \mathbf{v}_{\text{avg}} = \frac{1}{\sqrt{M}}(1, \dots, 1)^\top$ and ask what form of privacy can be achieved with a Gaussian probe under unitary local phase encoding. The answer is fundamentally different for two parties and for three or more parties. We start with a no-go theorem (Sec. III A), then turn to the exceptional two-party case (Sec. III B) and finally build a multipartite protocol (Sec. III C).

A. No-go for complete privacy with three or more parties

We first state our main no-go result, which shows that complete privacy of the average phase is impossible for finite-energy Gaussian networks with three or more parties.

Theorem 4. (No-go for complete average-phase privacy). No finite-energy M -mode Gaussian probe with $M \geq 3$

undergoing the local phase encoding of Eq. (10) can achieve complete privacy of the average phase with non-zero sensitivity. More explicitly, if $\mathbf{Q}$ satisfies

$$\text{range}(\mathbf{Q}) \subseteq \text{span}\{\mathbf{1}\}, \quad (14)$$

where $\mathbf{1} = (1, \dots, 1)^\top$, then $\mathbf{Q} = \mathbf{0}$.

Sketch of the proof. The full proof is given in Appendix F. We sketch the three steps here. (i) Unitarity of the encoding implies $\partial_u \hat{\rho} = i[\hat{G}_u, \hat{\rho}]$ with $\hat{G}_u = \sum_\mu u_\mu \hat{n}_\mu$, so $\mathbf{u} \in \ker \mathbf{Q}$ is equivalent to $[\hat{G}_u, \hat{\rho}] = 0$. Applying this to every $\mathbf{u} \in \mathcal{H}_0 := \{\mathbf{u} : \mathbf{1}^\top \mathbf{u} = 0\}$ forces $\hat{\rho}$ to be invariant under the entire zero-sum subgroup of local phase rotations. (ii) Translating this invariance to phase space using the symplectic action of phase rotations, one shows that the first moments must vanish, every diagonal covariance block must be rotationally symmetric ($\sigma_{\mu\mu} = \nu_\mu \mathbb{1}_2$), and—using the existence of a third mode $\ell \neq \mu, \nu$ to construct a zero-sum rotation that affects μ while leaving ν fixed—all off-diagonal blocks must vanish ($\sigma_{\mu\nu} = 0$ for $\mu \neq \nu$). (iii) The resulting state $\sigma = \bigoplus_\mu \nu_\mu \mathbb{1}_2$, $\bar{\mathbf{r}} = \mathbf{0}$ is invariant under every local phase rotation, not only the zero-sum ones. Hence the QFI vanishes identically, contradicting any assumption of finite average-phase sensitivity.

Importantly, the theorem is specific to the average-phase direction. It does not rule out rank-one Gaussian QFIs aligned with other parameter directions. For example, the finite-energy Gaussian probe $|\alpha\rangle\langle\alpha| \otimes |0\rangle\langle 0|^{\otimes(M-1)}$, with $\alpha \neq 0$, has $\mathbf{Q} = 4|\alpha|^2 \mathbf{e}_1 \mathbf{e}_1^\top$, under local phase encoding, and is therefore rank one but supported on the first coordinate. Thus the no-go result arises from requiring complete privacy of the average phase across three or more modes, not from rank one itself.

B. Complete privacy for two parties

We turn to the exceptional $M = 2$ case identified by Theorem 4 and show that the two-mode squeezed state (TMSS) provides complete average-phase privacy. The example also lets us introduce the main ingredients of interest, such as loss, displacement, measurement strategies, and the role of entanglement. In line with the no-side-information assumption $\mathbf{A}_2$, the two parties do not know their local phases prior to inference.

Consider a two-mode squeezed state (TMSS) undergoing local phase shifts θ_1 and θ_2 . In this simplest case, one may ask whether it is possible to estimate *only* the average phase. To make the scenario more realistic, we introduce noise prior to the phase encoding, modeled by a beam splitter with transmissivity η . For simplicity, we assume that both modes experience the same level of loss, even though in experimental implementations this symmetry may not hold. This assumption allows for a cleaner analytical treatment and captures the essential features of

the problem; in Appendix C, we show how the analysis generalizes when the losses differ. Under this symmetric-loss model, it can be shown that the quantum Fisher information matrix of the output state is given by

$$\mathbf{Q}(r, \eta) = \frac{\eta^2 \sinh^2 2r}{1 + 2(1 - \eta)\eta \sinh^2 r} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}. \quad (15)$$

This matrix is clearly of rank one, capturing the fact that only a single linear combination of the two local phases can be estimated. Diagonalizing $\mathbf{Q}(r, \eta)$, we find that it has a single nonzero eigenvalue $\lambda_{\text{avg}} = 2\eta^2 \sinh^2 2r / [1 + 2(1 - \eta)\eta \sinh^2 r]$, associated with the eigenvector $\mathbf{v}_{\text{avg}} = 1/\sqrt{2} (1, 1)^\top$ corresponding to the average phase $\phi_{\text{avg}} := 1/2 (\theta_1 + \theta_2)$. The second eigenvalue vanishes, $\lambda_{\text{rel}} = 0$, with the corresponding eigenvector $\mathbf{v}_{\text{rel}} = 1/\sqrt{2} (-1, 1)^\top$ linked to the relative phase $\phi_{\text{rel}} := 1/2 (\theta_2 - \theta_1)$. The vanishing QFI along this orthogonal direction confirms that the relative phase cannot be estimated. Since $\mathbf{v}_{\text{rel}} \in \ker \mathbf{Q}$ and both components of $\mathbf{v}_{\text{rel}}$ are nonzero, according to Definition 1, both phases θ_1 and θ_2 are private. In fact, since the QFI is rank one, we have complete privacy, and therefore $P(\mathbf{Q}, \mathbf{v}_{\text{avg}}) = 1$.

The two-mode setting falls outside the scope of Theorem 4 because there is no third mode available to force the off-diagonal block σ_{12} to vanish. The relative-phase symmetry that would otherwise be restrictive reduces to a one-dimensional subgroup, and the TMSS exploits the off-diagonal correlations that this symmetry leaves unconstrained. Although only the average phase remains estimable in the presence of noise, it is important to emphasize that the attainable precision degrades with η , as the QFI is reduced by a factor of $\eta^2 / [1 + 2(1 - \eta)\eta \sinh^2 r]$.

An interesting case arises when the modes are displaced before encoding the phases. Although this improves the estimation precision (as the quantum Fisher information increases), it compromises privacy. For simplicity, we set $\eta = 1$ and analyze what happens with the spectrum of the QFI. In contrast with the undisplaced case, the QFI is no longer rank one and has no zero eigenvalue: both the average-phase direction and directions with relative-phase content can carry finite Fisher information. The two eigenvalues can be written as $\lambda_{\pm} = f(\alpha_1, \alpha_2, r) \pm g(\alpha_1, \alpha_2, r)$, with eigenvectors that depend on the displacement pattern. We therefore avoid labelling them as purely “average” and “relative” eigenvalues except in symmetric limiting cases. When $\alpha_1 = \alpha_2 = 0$, we recover the undisplaced TMSS case, where the relative-phase direction is unobservable. As soon as the displacement pattern breaks the photon-number-correlation symmetry, the previously hidden direction acquires finite QFI. Physically, while the undisplaced TMSS is insensitive to opposite local phase shifts because of its perfect

photon-number correlations, displacements introduce local phase references and make relative-phase information observable. The loss of privacy by displacing the modes can be quantified by using Eq. (7), which gives us

$$P(\mathbf{Q}, \mathbf{v}_{\text{avg}}) = 1 - \frac{(\alpha_1^2 + \alpha_2^2) \cosh 2r + 2\alpha_1\alpha_2 \sinh 2r}{2(\alpha_1^2 + \alpha_2^2) \cosh 2r + \sinh^2 2r}, \quad (16)$$

where, without loss of generality, we assume that $\alpha_1, \alpha_2 \in \mathbb{R}$. Since $\alpha_1^2 + \alpha_2^2 \geq |2\alpha_1\alpha_2|$ and $\cosh 2r \geq |\sinh 2r|$, the numerator of the second term in Eq. (16) is non-negative and is strictly positive unless $\alpha_1 = \alpha_2 = 0$. Thus, displacing the modes before encoding the local phases invariably leads to a reduction in the privacy measure.

We now turn to the question of which measurements the parties are allowed to perform, and what the optimal protocol is for estimating the average phase. If we restrict attention to Gaussian measurements, it can be shown that the optimal strategy within the Gaussian toolbox involves the following scheme: after the local phase encoding, the two modes are interfered on a balanced beam splitter, followed by homodyne measurements in conjugate quadratures rotated by an angle ϕ (see Appendix C1). The optimal angle ϕ_{opt} is given by

$$\phi_{\text{opt}} = \frac{\theta_1 + \theta_2}{2} + \tan^{-1} \left(\frac{\eta \sinh 2r}{\sqrt{1 + 4(1 - \eta)\eta \sinh^2 r}} \right). \quad (17)$$

However, this dependence of ϕ_{opt} on the unknown average phase poses a practical challenge. This apparent circularity is resolved by standard adaptive metrology: a short pre-run with heterodyne (or fixed-angle homodyne) detection provides a coarse estimate of ϕ_{avg} . The local oscillators are then iteratively steered towards ϕ_{opt} until the classical Fisher information is maximized. In the lossless case, the resulting Fisher information saturates the quantum benchmark, while under loss, it does not generally attain the QFI. In the regime where phase shifts are small, the average can be neglected, and the optimal angle becomes effectively independent of the unknown parameter, removing the need for adaptive alignment.

Finally, let us consider the role of entanglement for privacy. This naturally leads to a comparison between the previous scenario and the case in which the two-mode squeezed state is replaced by two single-mode squeezed states. Following the same protocol (and assuming $\eta = 1$ and $\alpha_1 = \alpha_2 = 0$), it is straightforward to show that the QFI is $\mathcal{Q}(r) = 2 \sinh^2(2r) \mathbb{1}_2$, with degenerate spectrum $\lambda_{\text{avg/rel}} = 2 \sinh^2(2r)$. Hence $\ker(\mathbf{Q}) = \mathbf{0}$ and, by Definition 1, there exists no nonzero vector $\mathbf{v}$ with $v_j \neq 0$ lying in the kernel. In particular, no component θ_j is private. This can be seen directly from the privacy measure: for both the average-phase direction $\mathbf{v}_{\text{avg}}$ and

the relative-phase direction $\mathbf{v}_{\text{rel}}$, we have $P(\mathbf{Q}, \mathbf{v}_{\text{avg}}) = P(\mathbf{Q}, \mathbf{v}_{\text{rel}}) = 1/2$. Thus only half of the available information aligns with the chosen public function, and the remaining half leaks into the orthogonal combination. Equivalently, the scalar QCRB (4) shows that both combinations are estimated with identical precision. By contrast with the TMSS case, where $\mathbf{Q}$ is rank-one and concentrates all information along the average-phase direction, two independent single-mode squeezers distribute information uniformly across all phase combinations. This comparison highlights the role of the shared TMSS correlations: the independent squeezers retain sensitivity to the collective target, but their full-rank QFI provides neither complete nor component privacy.

C. Weak privacy in a quantum network

Theorem 4 rules out complete average-phase privacy for $M \geq 3$, since any Gaussian probe whose QFI has $\text{range}(\mathbf{Q}) = \text{span}\{\mathbf{v}_{\text{avg}}\}$ must have $\mathbf{Q} = \mathbf{0}$. For three or more parties, the relevant goal is therefore weaker: every individual phase should remain private, while the normalized QFI becomes increasingly concentrated along the average-phase direction as the squeezing increases. We now introduce an experimentally feasible protocol with exactly these properties. The protocol proceeds as follows (see Fig. 3 for a pictorial overview):

1. A two-mode squeezed state is distributed among M modes using a beam splitter network, with vacuum states injected into the unused input ports.
2. Each output mode undergoes a local phase shift θ_i , where $i \in \{1, \dots, M\}$.
3. Each party performs a local measurement, and the broadcast outcomes are processed centrally to estimate the average phase.

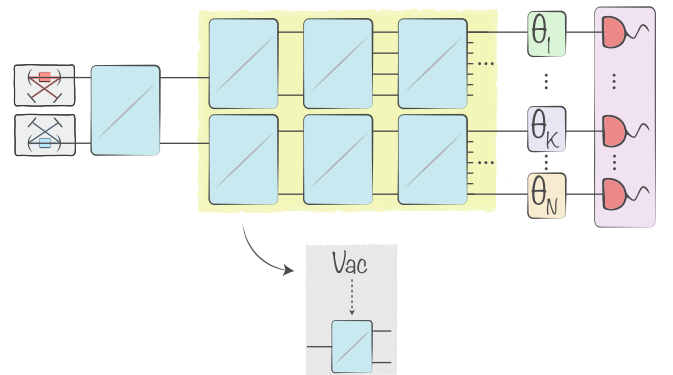


FIG. 3. Protocol. Two orthogonally squeezed states are generated by optical parametric oscillator (OPOs) and mixed at a central beam splitter to produce a two-mode squeezed state. This is symmetrically distributed via a recursive beam splitter network (yellow area), where each layer mixes modes with vacuum, doubling their number. The resulting state then undergoes local phase shifts $\{\theta_1, \dots, \theta_M\}$, followed by local measurements.

The choice of a two-mode squeezed state is motivated by the two-party example of Sec. III B. There, privacy comes from a symmetry of the TMSS: the two modes always contain matching photon-number fluctuations, so opposite phase shifts on the two modes cannot be distinguished. The beam-splitter network used below only redistributes the optical fields among more parties. It does not destroy this correlation between the two original input modes. As a result, one collective phase direction remains unobservable after the state is distributed, and this unobservable direction is what makes every individual phase weakly private. This would not happen if the input resource was a single-mode squeezed vacuum sent through the same balanced beam-splitter network, with vacuum in the unused input ports. In that case, the network would simply spread one squeezed mode over many parties. There would be no second, photon-number-correlated input mode to provide a hidden opposite phase symmetry. Consequently, all local phase directions would carry some information, the QFI would have no nontrivial kernel, and no individual phase would be private according to Definition 1. Thus, weak privacy is not produced by the beam-splitter network alone. It comes from the TMSS symmetry that the network preserves while distributing the state.

As our goal is to analyze the privacy of the protocol, we first construct the quantum Fisher information matrix for the setting at hand. The following lemma gives its explicit form:

Lemma 5. (Beam-splitter-tree QFI). Consider a two-mode squeezed state split into 2^N modes by a balanced 50: 50 beam splitter network. Encoding local phases $\theta = (\theta_1, \dots, \theta_M)$ via $\hat{U}(\theta) = \bigotimes_{\mu=1}^M e^{i\theta_\mu \hat{n}_\mu}$, the corresponding quantum Fisher information matrix $\mathcal{Q}$ is independent of θ and can be written in the projector form

$$\mathcal{Q} = \frac{\cosh 2r - 1}{2^{N-2}} (\mathbb{1}_M - \Pi_+ - \Pi_0) + \frac{\cosh 4r - 1}{2^{N-1}} \Pi_+, \quad (18)$$

where $\Pi_+ = \mathbf{1}\mathbf{1}^\top/M$ and $\Pi_0 = \mathbf{s}\mathbf{s}^\top/M$ with $\mathbf{1} = (1, \dots, 1)^\top$ and $\mathbf{s} = (\underbrace{1, \dots, 1}_{\frac{M}{2}}, \underbrace{-1, \dots, -1}_{\frac{M}{2}})^\top$.

With an explicit characterization of the quantum Fisher information matrix in hand, Definition 1 implies that its eigenvalues determine the achievable privacy. The following theorem gives the spectrum of $\mathcal{Q}$:

Theorem 6. (Spectrum and eigenmodes of the QFI). The eigenvalues of the quantum Fisher information matrix $\mathcal{Q}$ characterized by Lemma 5 are

$$\lambda(\mathcal{Q}) = \left\{ 0, \underbrace{\frac{\cosh 2r - 1}{2^{N-2}}, \dots, \frac{\cosh 2r - 1}{2^{N-2}}}_{M-2 \text{ times}}, \frac{\cosh 4r - 1}{2^{N-1}} \right\}. \quad (19)$$

The corresponding orthonormal eigenbasis is given by:

- i. Zero eigenvalue: $\mathbf{v}_0 = \frac{\mathbf{s}}{\sqrt{M}}$.
- ii. Degenerate eigenvalue: $\mathcal{W} = \{\mathbf{w} : \mathbf{1}^\top \mathbf{w} = 0, \mathbf{s}^\top \mathbf{w} = 0\}$.
- iii. Largest eigenvalue: $\mathbf{v}_{\text{avg}} = \frac{\mathbf{1}}{\sqrt{M}}$.

The null direction $\mathbf{v}_0 = \frac{\mathbf{s}}{\sqrt{M}}$ has a transparent symmetry interpretation. It corresponds to applying the same phase shift to all modes descended from one input arm of the initial TMSS and the opposite phase shift to all modes descended from the other arm. Because the beam-splitter tree is passive, the corresponding generator collapses to $\hat{G}_0 = \frac{1}{\sqrt{M}}(\hat{n}_A - \hat{n}_B)$, where $\hat{n}_A = \sum_{j \in A} \hat{n}_j$ and $\hat{n}_B = \sum_{j \in B} \hat{n}_j$ are the total photon numbers on the two branches. A two-mode squeezed vacuum has perfect photon-number correlations, so $\text{var}(\hat{n}_A - \hat{n}_B) = 0$. The QFI along $\mathbf{v}_0$ therefore vanishes by symmetry. Equivalently, the state is invariant under opposite phase rotations of the two TMSS branches, and the beam-splitter network preserves this symmetry. The zero eigenvalue in Eq. (19) is thus a direct consequence of the input symmetry rather than an accidental cancellation.

The spectrum in Theorem 6 admits a clear metrological interpretation. There are three distinct sectors: one zero eigenvalue (a single direction with vanishing sensitivity), an $(M-2)$ -dimensional shot-noise-limited subspace with eigenvalues scaling linearly with the mean photon number, and a unique enhanced direction whose eigenvalue includes a quadratic contribution in the photon number, thus providing a Heisenberg scaling precision benchmark. In other words, among all independent phase combinations, only one collective mode is metrologically special, while all others remain shot-noise limited. A detailed derivation of the photon-number scaling of these eigenvalues is provided in Appendix D4.

Combining Lemma 5 with Theorem 6, we can now determine the privacy properties of this protocol. This is done via the following corollary:

Corollary 7. (Private components). For a TMSS split into $M = 2^N$ modes via a balanced 50: 50 beam splitter network, with local phases encoded through phase shifts:

- (i) The kernel of $\mathcal{Q}$ is one-dimensional, with $\mathbf{v}_0 \in \ker \mathcal{Q}$, so there exists a single unobservable direction and the scheme exhibits weak privacy.
- (ii) Since every entry of $\mathbf{s}$ is nonzero, each parameter θ_j is individually private.

- (iii) The QFI is not rank-one: there are $M - 2$ degenerate eigenvalues $(\cosh 2r - 1)/2^{N-2}$ associated with $\mathcal{W}$. Hence complete privacy does not hold.

Item (iii) is also a structural consequence of Theorem 4: complete privacy is impossible for $M \geq 3$ Gaussian probes with unitary phase encoding, so any concrete protocol can at best achieve the weak privacy described in items (i)–(ii). The proofs of these three results are given in Appendix D. We also provide an efficient *Mathematica* notebook that constructs the covariance matrix of the beam splitter tree, the quantum Fisher information matrix, and its eigenvalues for an arbitrary number of nodes in the network—along with many other results concerning privacy in CV systems [47]. The above results assume a specific resource state, namely a two-mode squeezed state, and a specific protocol, consisting of a beam-splitter network followed by local phase encoding. For a generic pure state produced by a Gaussian protocol and subjected to local phase shifts, the QFI can be computed using Lemma 2. In the case of interest—where $|\psi_0\rangle$ is a two-mode squeezed state distributed through a beam splitter network—Lemma 2 recovers Lemma 5 (and vice versa).

We summarize the message of this section. For $M = 2$ the TMSS achieves complete privacy, and Theorem 4 closes the door on this for any $M \geq 3$. When the TMSS is distributed among more parties via the beam-splitter tree, every individual phase remains private (Corollary 7), but certain orthogonal combinations leak; the leaked information is, however, insufficient to reconstruct any individual phase under the no-side-information assumption $\mathbf{A}_2$. In linear-algebra terms, the encoded data leave an under-determined affine family of compatible parameter vectors $\boldsymbol{\theta} + \ker \mathbf{Q}$, so no individual component is identifiable from the public record alone without additional side information. We now turn to a quantitative analysis of these results.

IV. PRIVACY PERFORMANCE AND IMPERFECTIONS

For $M \geq 3$, complete average-phase privacy cannot be achieved by finite-energy Gaussian probes (Theorem 4). However, privacy at the level of individual phases remains guaranteed for the TMSS-tree protocol (Corollary 7). We now analyze the privacy performance of this protocol under displacement and loss and compare it with selected alternative Gaussian resources.

In Fig. 4 we plot the two nonzero eigenvalues of the QFI [Eq. (19)] as functions of the squeezing parameter on a log-log scale, for different values of M (colors ranging from red to black). The left and right panels show the largest and smallest nonzero eigenvalues, respectively. As the squeezing increases, the dominant eigenvalue grows as $\cosh 4r$ while the subdominant eigenvalue grows as $\cosh 2r$, both diverge in absolute terms, but the ratio between them grows as $\cosh 4r / \cosh 2r \sim e^{2r}$ at large r . Consequently, the fraction of the total Fisher information

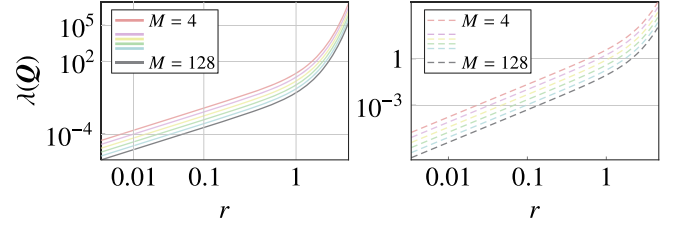


FIG. 4. Quantum Fisher information spectrum. Log-log plot of the eigenvalues of the quantum Fisher information matrix $\lambda(\mathbf{Q})$ as a function of the squeezing parameter r , for different numbers of modes $M = 2^N$. The largest eigenvalue is shown with solid lines, while the smallest nonzero eigenvalue is shown with dashed lines. As M increases, the spectral gap between the two eigenvalues widens, highlighting how the distribution of information across phase directions depends on both squeezing and network size. The total number of photons (and hence the total metrological resource) is conserved; splitting the state among more modes spreads these photons more thinly across the network, so each local phase shift affects fewer photons and the sensitivity per parameter direction decreases.

lying outside the average-phase direction vanishes asymptotically, and the normalized spectrum approaches the rank-one limit, even though no eigenvalue is in fact suppressed. With a fixed total mean photon number, increasing the number of modes M spreads the photons across more parameters; as a result, each local phase receives fewer photons and the shot-noise-limited sensitivity per direction decreases.

Applying Theorem 3, one can get a closed-form expression for the privacy as a function of the number of parties ($M = 2^N$) in the average phase estimation, namely we have that

$$P(\mathbf{Q}, \mathbf{v}_{\text{avg}}) = 1 - \frac{2^N - 2}{[(2^N - 1) + \cosh 2r]} \quad \text{for } r > 0, \quad (20)$$

Reaching $P = 1$ in the multi-party setting would require the unphysical infinite-squeezing limit, consistent with Theorem 4. At first sight, this behavior may seem paradoxical. Although the privacy measure falls approximately as $1/M$, the QFI always contains a strictly zero eigenvalue, ensuring that at least one linear combination of local phases remains completely hidden. This reflects the structure of the beam splitter network. Each added layer doubles the number of output modes and enlarges the phase subspace orthogonal to the protected direction. Besides the fully hidden branch-imbalance vector $\mathbf{s} = (\underbrace{1, \dots, 1}_{M/2}, \underbrace{-1, \dots, -1}_{M/2})^\top$, defined in Lemma 5, the

QFI has an $(M - 2)$ -dimensional degenerate eigenspace $W = \{w \in \mathbb{R}^M : \mathbf{1}^\top w = 0, \mathbf{s}^\top w = 0\}$. Writing $A = \{1, \dots, \frac{M}{2}\}$ and $B = \{\frac{M}{2} + 1, \dots, M\}$ for the two branches of the tree, the conditions $\mathbf{1}^\top w = 0$ and $\mathbf{s}^\top w = 0$ are

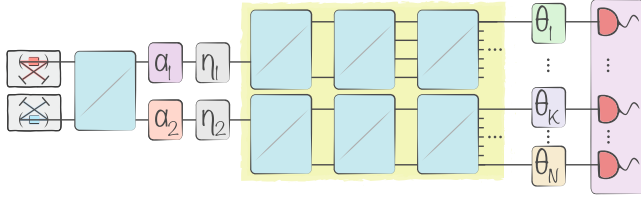


FIG. 5. Displacement and loss. The two-mode squeezed state is first displaced by amounts α_1 and α_2 and then subjected to a loss channel modeled by beam splitters with transmissivities η_1 and η_2 , respectively. Subsequently, the modes undergo the beam splitter network, after which local phases are encoded.

equivalent to $\sum_{j \in A} w_j = 0, \sum_{j \in B} w_j = 0$. Thus W consists of phase contrasts within each branch, such as $e_1 - e_2$ or $e_{\frac{M}{2}+1} - e_{\frac{M}{2}+2}$, rather than contrasts between the two branches. All directions in W have the same finite eigenvalue $(\cosh 2r - 1)/2^{N-2}$. With r held fixed, the total Fisher information must be distributed across more directions, so the share associated with the average phase diminishes. Henceforth we restrict attention to the four-mode instance $M = 4$, the smallest network that already displays all qualitative features (a single fully hidden direction, plus degenerate orthogonal sensing directions) and is experimentally realizable. Using Eq. (20), $P_4(r) := 1 - \frac{2}{3 + \cosh 2r}$.

We now consider a slightly more general scenario by introducing displacement operations on both modes before they are sent through the beam splitter network (see Fig. 5). First, as in the two-mode case, displacements remove the strictly zero eigenvalue of the QFI, so that no parameter direction remains completely hidden. However, the smallest eigenvalue can remain very small (ϵ -close to zero). Second, by Theorem 3, the privacy measure when the TMSS is split into four modes is $P(\mathbf{Q}, \mathbf{v}) = P_4(r) - f(r, \alpha_1, \alpha_2)$, where $f(r, \alpha_1, \alpha_2) \geq 0$ quantifies the reduction in privacy due to the displacements.

In the first panel of Fig. 6 we examine privacy in the absence of loss ($\eta = 1$) while displacing the TMSS by $|\alpha| = |\alpha_2 - \alpha_1|$ in phase space. In the plotted curves we restrict to the displacement path specified in the numerical calculation, so that $|\alpha|$ denotes the chosen relative displacement amplitude rather than a complete parameterization of the two-dimensional displacement space. The privacy measure decreases with increasing $|\alpha|$, although it asymptotically approaches one as $r \rightarrow \infty$. Since displacement is a resource for parameter estimation, the reduction in privacy arises from information leakage at the level of the encoded state: displacements break the symmetry in phase space and individual phases are imprinted in the first moments. Operationally, any unintended displacement can be diagnosed by estimating the first moments of each mode (which ideally vanish in the undisplaced protocol).

Correspondingly, the scalar Fisher information $(\mathbf{v}^T \mathbf{Q} \mathbf{v})^{-1}$ (bottom panel of Fig. 6) increases with $|\alpha|$. Importantly, values of P close to 1 should not by

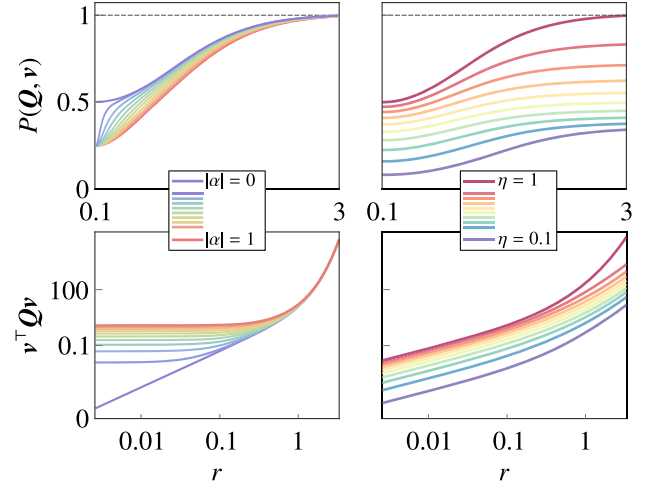


FIG. 6. Privacy under displacement and loss. Top panels: privacy for different values of $|\alpha| = |\alpha_2 - \alpha_1|$ in the absence of loss (left), and privacy in the presence of a loss channel with efficiency η for fixed $|\alpha| = 0$ (right). Bottom panels: effective scalar QFI $(\mathbf{v}_{\text{avg}}^T \mathbf{Q} \mathbf{v}_{\text{avg}})^{-1}$ for the average-phase target, which is in range $(\mathbf{Q})$ throughout the plotted regimes, so the pseudoinverse expression is well defined.

themselves be read as “more secrecy.” When overall sensitivity is depleted, $P \rightarrow 1$ can simply indicate that nearly all information has been erased rather than genuinely hidden. In the second panel we replace displacement with a loss channel of transmissivity η . Loss degrades the privacy measure, but this reduction does not arise from information leakage—the zero eigenvalue of the QFI persists. Rather, it reduces the fraction of the total Fisher information aligned with the target. A possible way to improve privacy in the presence of loss is to allow finite displacement and optimize over $|\alpha|$, increasing precision at the cost of partially sacrificing privacy.

Having characterized the impact of imperfections in the TMSS-based protocol, we now ask whether alternative Gaussian states might offer improved or comparable privacy. In particular, we explore whether continuous-variable analogs of graph states—linear cluster states generated via CZ operations—can support private estimation of the average phase. We compare the privacy of cluster states with that of both the TMSS-split network and separable squeezed product states. We benchmark the privacy of different Gaussian states under average phase estimation (see Fig. 7). A TMSS distributed symmetrically via beam splitters concentrates an increasing fraction of the Fisher information along the target direction, leading to $P \rightarrow 1$ in the large-squeezing limit even though the off-target eigenvalues do not vanish absolutely. In contrast, cluster states do not support private estimation: their privacy measure asymptotically converges to the separable-state baseline $P = \frac{1}{4}$. Increasing the CZ coupling strength does not improve privacy and, in fact, leads to

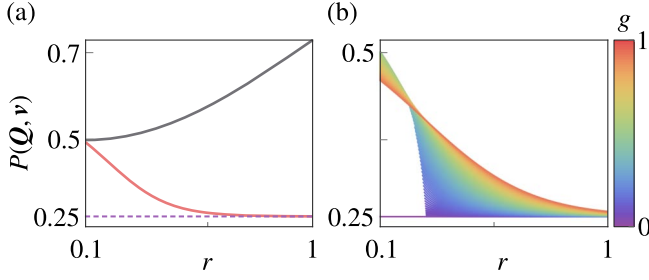


FIG. 7. Privacy comparison. (a) Privacy $P(Q, \mathbf{v}_{\text{avg}})$ as a function of r for three states: TMSS distributed via a symmetric beam splitter network (black), a linear cluster state on four parties via sequential CZ operations on $\{(1, 2), (2, 3), (3, 4)\}$ at the optimal coupling $g_{\text{opt}} \approx 0.88$ (red), and a product of single-mode squeezed states (dashed). (b) Privacy of the cluster state for various g versus r .

greater information leakage about individual parameters, suggesting a fundamental incompatibility between the position-position correlations introduced by CZ operations and the number-based phase encoding used here. Whether the TMSS-tree protocol is optimal among all Gaussian probes under the no-go constraint of Theorem 4 remains an open question. For the specific protocol considered here, however, we provide both analytical and numerical evidence that it is near-optimal within the family of Gaussian resources we tested.

V. CONCLUSION AND OUTLOOK

We have introduced and analyzed an information-theoretic characterization of privacy for continuous-variable sensor networks. Our framework is based on unobservable directions, namely vectors lying in the kernel of the QFI, and provides an operational way to assess privacy at the level of individual components under the prescribed-protocol and no-side-information assumptions $\mathbf{A}_1$ to $\mathbf{A}_4$. The central structural result is Theorem 4, which states that, under unitary local phase encoding, complete privacy of the average phase is impossible at finite energy for three or more modes. The two-mode squeezed state is the exceptional Gaussian case that achieves complete privacy. For the TMSS distributed over $M = 2^N$ modes, we derived a closed-form projector expression for the QFI in Lemma 5, obtained its full spectrum and eigenmodes in Theorem 6, and translated these results into operational privacy statements in Corollary 7. The protocol has a single unobservable direction and makes every local phase individually private, although complete privacy is not attained at finite squeezing. We also obtained general closed-form expressions for the QFI of arbitrary pure multimode Gaussian states undergoing local phase shifts in Lemma 2 and for the privacy measure $P(Q, \mathbf{v}_{\text{avg}})$ in Theorem 3.

We further analyzed two practically relevant scenarios. Displacements enhance estimation precision by imprinting phases into the first moments but simultaneously remove the zero eigenvalue of the QFI, destroying privacy at the component level. Optical loss preserves the zero eigenvalue, so no individual phase becomes identifiable, but it reduces the fraction of the total Fisher information aligned with the target direction, lowering the privacy measure. A comparative study revealed that alternative Gaussian resources, such as four-mode cluster states or independent single-mode squeezers, perform worse than the TMSS-tree protocol within the family we tested. A natural question under the no-go constraint of Theorem 4 is to identify the optimal protocol among experimentally friendly Gaussian resources.

The privacy guarantees of this work rely on the access-controlled encoding assumption $\mathbf{A}_2$ and on the adversarial model $\mathbf{A}_4$: each party can use only the public broadcast and the quantum systems in its possession to infer information about the local phases, has no additional query access to any encoding channel, and does not know any raw value θ_μ directly. If adversaries are instead allowed to know their own raw phases, or to interrogate their encoding channels with auxiliary probes, the privacy criterion used here is no longer sufficient. Indeed, for the TMSS-tree protocol the QFI has a one-dimensional kernel generated by a vector with nonzero support on every component. Fixing even one component of $\boldsymbol{\theta}$ then removes the remaining ambiguity along this kernel direction and can reveal the other components. A natural strengthening, which we leave for future work, is conditional privacy. In this stronger sense, θ_j would remain private against an adversarial subset $S \not\ni j$ if there exists a kernel direction $\mathbf{w} \in \ker Q$ such that $w_j \neq 0$ while $w_i = 0$ for every $i \in S$. Designing continuous-variable protocols whose QFI kernels satisfy this stronger condition is an open problem. While our analysis assumes an honest setting, this is an idealization that may not hold in practical network deployments. Another extension is therefore to incorporate a certification layer, enabling participants to verify *in situ* that the distributed resource is sufficiently close to the intended state. In the discrete-variable regime, Shettell *et al.* [20] have shown how stabilizer-based tests can certify GHZ-type states. More recently, Descamps and Markham [42] extended this result to continuous-variable graph states, developing noise-tolerant verification routines. An open problem is to develop a certification protocol tailored to our specific scheme.

Finally, our scheme can be feasibly implemented using a source of two-mode squeezed states, an array of beam splitters, and homodyne detectors. Two single-mode squeezed states can be generated via parametric down-conversion [48] or four-wave mixing [49] and interfered on a balanced beam splitter to produce a two-mode squeezed vacuum. This TMSS is then distributed to four

parties by an additional beam-splitter network. Each party's local phase is imprinted by a channel that the party does not control, after which homodyne measurements of appropriately chosen quadratures on each mode are performed to reconstruct the covariance matrix of the state. The state preparation, distribution, and detection stages thus rely only on well-established optical components. We emphasize, however, that the Heisenberg-scaling precision discussed in this work is a benchmark defined under unrestricted measurements: constructing a strictly local measurement strategy that attains it for $M \geq 3$, or quantifying the unavoidable gap, remains an important open step toward a fully distributed implementation.

ACKNOWLEDGMENTS

A. O. J. would like to thank Mohammad Mehboudi for the helpful discussions. The authors acknowledge financial support from the EU Horizon Europe (QSNP, grant no. 101114043 & CLUSTEC, grant no. 101080173 & ClusterQ, grant no. 101055224), NNF project CBQS (NNF 24SA0088433), the Danish National Research Foundation grant bigQ (DNRF 142). M. T. acknowledges JST Moonshot R&D (JPMJMS226C and JPMJMS2061), JST CRONOS (JPMJCS24N6), and JST ASPIRE (JPMJAP2427). S. W. M. and D. M. acknowledge support from the ANR project EQUINE (ANR-23-QUAC-0001). The result that complete privacy, for more than two parties, cannot be obtained with Gaussian resources (Theorem 4) has been obtained independently by different methods by J. L. Pereira and D. Markham in [50].

DATA AVAILABILITY

There are no publicly available research data or software supporting this manuscript. Requests for further information or data should be sent to the authors.

APPENDIX A: UNOBSERVABILITY & PRIVACY

In this appendix we prove Proposition 1. We first present a lemma giving equivalent characterizations of unobservability at regular points of the quantum statistical model; the unitary phase-encoding family used in the main text falls in this class, as discussed below Definition 1.

Lemma 8. (Equivalent criteria for unobservability at regular points). Suppose the multiparameter statistical model is regular at θ , in the sense that $\hat{\rho}(\theta)$ has locally constant rank and the SLDs are well defined on $\text{supp}(\hat{\rho})$. Let $\mathbf{Q}$ be the QFI with entries $Q_{\mu\nu} = \frac{1}{2} \text{tr}[\hat{\rho}\{\hat{L}_{\theta_\mu}, \hat{L}_{\theta_\nu}\}]$, where $\hat{L}_{\theta_\mu}$ are the SLDs. Then, for any real vector $\mathbf{u} \in \mathbb{R}^M$, the following are equivalent:

- (i) $\partial_{\mathbf{u}}\hat{\rho} = 0$,
- (ii) $\hat{L}_{\mathbf{u}} := \sum_{\mu} u_{\mu} \hat{L}_{\theta_\mu} = 0$ on $\text{supp}(\hat{\rho})$,
- (iii) $\mathbf{u} \in \ker \mathbf{Q}$.

Proof. Linearity of the SLD equation gives $2\partial_{\mathbf{u}}\hat{\rho} = \hat{\rho}\hat{L}_{\mathbf{u}} + \hat{L}_{\mathbf{u}}\hat{\rho}$, $\hat{L}_{\mathbf{u}} := \sum_{\mu} u_{\mu} \hat{L}_{\theta_\mu}$. Moreover, $\mathbf{u}^\top \mathbf{Q} \mathbf{u} = \text{tr}(\hat{\rho}\hat{L}_{\mathbf{u}}^2) \geq 0$. Thus $\mathbf{u} \in \ker \mathbf{Q}$ if and only if $\text{tr}(\hat{\rho}\hat{L}_{\mathbf{u}}^2) = 0$, which is equivalent to $\hat{L}_{\mathbf{u}} = 0$ on $\text{supp}(\hat{\rho})$. The SLD equation then gives $\partial_{\mathbf{u}}\hat{\rho} = 0$ on the support. At regular points the rank of $\hat{\rho}(\theta)$ is locally constant, so the SLD equation represents the full derivative without additional singular terms from eigenvalues emerging out of zero. Hence $\partial_{\mathbf{u}}\hat{\rho} = 0$. Conversely, if $\partial_{\mathbf{u}}\hat{\rho} = 0$, then the SLD equation gives $\hat{\rho}\hat{L}_{\mathbf{u}} + \hat{L}_{\mathbf{u}}\hat{\rho} = 0$. In an eigenbasis of $\hat{\rho}$, with eigenvalues p_a , this reads $(p_a + p_b)(L_{\mathbf{u}})_{ab} = 0$. Whenever at least one of a, b belongs to the support of $\hat{\rho}$, one has $p_a + p_b > 0$, and therefore $(L_{\mathbf{u}})_{ab} = 0$. Hence $\hat{L}_{\mathbf{u}} = 0$ on $\text{supp}(\hat{\rho})$, and $\mathbf{u}^\top \mathbf{Q} \mathbf{u} = \text{tr}(\hat{\rho}\hat{L}_{\mathbf{u}}^2) = 0$. Since $\mathbf{Q} \geq 0$, this is equivalent to $\mathbf{u} \in \ker \mathbf{Q}$. ■

APPENDIX B: PRIVACY MEASURE IN GHZ, W, AND PRODUCT STATES

To illustrate the notion of privacy, consider a simple phase-estimation protocol. Specifically, three parties sharing a state $|\Psi\rangle$ each locally encode a phase θ_j by applying the unitary operation $U(\theta_j) = |0\rangle\langle 0| + e^{i\theta_j}|1\rangle\langle 1|$. Our goal is to assess privacy when the parties attempt to estimate the average phase $\theta_{\text{avg}} = (\theta_1 + \theta_2 + \theta_3)/3$. This can be achieved by computing $P(\mathbf{Q}, \mathbf{v}_{\text{avg}})$, where in this case $\mathbf{v}_{\text{avg}} = \frac{1}{\sqrt{3}}(1, 1, 1)$. Consequently, the problem reduces to calculating the quantum Fisher information matrix $\mathbf{Q}$ with respect to the average phase. As we are dealing with pure states, the QFI is simply given by

$$\mathbf{Q}_{\mu\nu}(\theta) = 4\text{Re}[\langle \partial_{\theta_\mu} \Psi(\theta) | \partial_{\theta_\nu} \Psi(\theta) \rangle - \langle \partial_{\theta_\mu} \Psi(\theta) \rangle \langle \Psi(\theta) | \partial_{\theta_\nu} \Psi(\theta) \rangle]. \quad (\text{B1})$$

To highlight the nontrivial nature of $P(\mathbf{Q}, \mathbf{v}_{\text{avg}})$, we consider two different state preparations undergoing the local encoding. Namely,

$$|\text{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \xrightarrow{U(\theta)} |\Phi_{\text{GHZ}}(\theta)\rangle = \frac{1}{\sqrt{2}}(|000\rangle + e^{i(\theta_1+\theta_2+\theta_3)}|111\rangle). \quad (\text{B2})$$

$$|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle) \xrightarrow{U(\theta)} |\Phi_+(\theta)\rangle = \frac{1}{\sqrt{3}}(e^{i\theta_3}|001\rangle + e^{i\theta_2}|010\rangle + e^{i\theta_1}|100\rangle). \quad (B3)$$

These two cases illustrate opposite extremes: the GHZ state allows complete privacy for the average phase, whereas the W state is blind to the average phase. To see this, we compute the quantum Fisher information for each state:

$$\mathbf{Q}_{\text{GHZ}} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \quad \mathbf{Q}_W = \frac{4}{9} \begin{pmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{pmatrix}. \quad (B4)$$

From their quantum Fisher information, we observe that $\mathbf{Q}_{\text{GHZ}}$ is a rank-one matrix proportional to $\mathbf{v}_{\text{avg}} \mathbf{v}_{\text{avg}}^T$. By contrast, $\mathbf{Q}_W$ has rank two and $\ker \mathbf{Q}_W = \text{span}\{(1, 1, 1)^T\}$. Thus the average-phase direction $\mathbf{v}_{\text{avg}} = \frac{1}{\sqrt{3}}(1, 1, 1)^T$ lies in the kernel of $\mathbf{Q}_W$, so the average phase is completely inaccessible from this state. Nevertheless, since the null vector has nonzero support on every component, each individual phase is private in the sense of Definition 1. We therefore have $P(\mathbf{Q}_{\text{GHZ}}, \mathbf{v}_{\text{avg}}) = 1$ and $P(\mathbf{Q}_W, \mathbf{v}_{\text{avg}}) = 0$.

As a final case, we now consider the scenario in which the parties share product states and each encodes the local phase, leading to

$$|+3\rangle = \left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \right]^{\otimes 3} \xrightarrow{U(\theta)} |\Phi_+(\theta)\rangle = \bigotimes_{j=1}^3 \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta_j}|1\rangle). \quad (B5)$$

In this case, the quantum Fisher information is simply $\mathbf{Q}_+ = \mathbb{1}_3$. This implies that each phase θ_j can be independently and optimally estimated. Nothing is hidden—all functions are accessible, as the QFI is full rank and every direction in parameter space is estimable. Even though the product state leaks all information (i.e., there is no privacy in the conventional sense), the privacy measure $P(\mathbf{Q}, \mathbf{v})$ is still nonzero—specifically, $P(\mathbf{Q}, \mathbf{v}_{\text{avg}}) = \frac{1}{3}$. The fact that P is not zero reflects that the desired function is indeed accessible, but information about other functions is also present.

APPENDIX C: MINIMAL SCENARIO FOR PRIVACY

Consider a scenario in which two parties share a two-mode squeezed state, characterized by the covariance matrix

$$\boldsymbol{\sigma} = \frac{1}{2} \begin{pmatrix} \cosh 2r & 0 & -\sinh 2r & 0 \\ 0 & \cosh 2r & 0 & \sinh 2r \\ -\sinh 2r & 0 & \cosh 2r & 0 \\ 0 & \sinh 2r & 0 & \cosh 2r \end{pmatrix}, \quad (C1)$$

with a first-moment vector given by $\bar{\mathbf{r}} = \mathbf{0}$. To maintain generality, one can assume an imperfect state preparation by sending the two-mode squeezed state through a Gaussian loss channel. This can be modeled by coupling both modes to a vacuum mode via a beam splitter with transmissivity η . After this transformation, the covariance matrix of the output state is given by:

$$\boldsymbol{\sigma}_{\text{loss}} = \frac{1}{2} \begin{pmatrix} 1 + 2\eta \sinh^2 r & 0 & -\eta \sinh 2r & 0 \\ 0 & 1 + 2\eta \sinh^2 r & 0 & \eta \sinh 2r \\ -\eta \sinh 2r & 0 & 1 + 2\eta \sinh^2 r & 0 \\ 0 & \eta \sinh 2r & 0 & 1 + 2\eta \sinh^2 r \end{pmatrix}, \quad (C2)$$

Assuming that both parties encode a phase θ_j via a phase shift, the encoded covariance matrix takes the following form:

$$\boldsymbol{\sigma}_\theta = \frac{1}{2} \begin{pmatrix} 1 + 2\eta \sinh^2 r & 0 & -\eta \cos(\theta_1 + \theta_2) \sinh 2r & -\eta \sin(\theta_1 + \theta_2) \sinh 2r \\ 0 & 1 + 2\eta \sinh^2 r & -\eta \sin(\theta_1 + \theta_2) \sinh 2r & \eta \cos(\theta_1 + \theta_2) \sinh 2r \\ -\eta \cos(\theta_1 + \theta_2) \sinh 2r & -\eta \sin(\theta_1 + \theta_2) \sinh 2r & 1 + 2\eta \sinh^2 r & 0 \\ -\eta \sin(\theta_1 + \theta_2) \sinh 2r & \eta \cos(\theta_1 + \theta_2) \sinh 2r & 0 & 1 + 2\eta \sinh^2 r \end{pmatrix}, \quad (C3)$$

The SLDs can be directly obtained when $\eta = 1$. However, for an arbitrary η , the calculation is not as straightforward. Nonetheless, we can construct an ansatz for the SLD. More precisely, both symmetric logarithmic derivatives are identical and given by:

$$\mathcal{L}_{\theta_{1,2}} = \frac{\sinh 2r}{2 + 4\eta(1-\eta)\sinh^2 r} \begin{pmatrix} 0 & 0 & \sin(\theta_1 + \theta_2) & -\cos(\theta_1 + \theta_2) \\ 0 & 0 & -\cos(\theta_1 + \theta_2) & -\sin(\theta_1 + \theta_2) \\ \sin(\theta_1 + \theta_2) & -\cos(\theta_1 + \theta_2) & 0 & 0 \\ -\cos(\theta_1 + \theta_2) & -\sin(\theta_1 + \theta_2) & 0 & 0 \end{pmatrix}. \quad (\text{C4})$$

Observe that Eq. (C4) satisfies $\mathcal{D}_\sigma(\mathcal{L}_{\theta_{1,2}}) = 2\partial_{\theta_1, \theta_2} \sigma$.

Thus, it is straightforward to show that the quantum Fisher information matrix in this case is rank-1 and given by

$$\mathcal{Q} = \frac{\eta^2 \sinh^2 2r}{1 + 2(1-\eta)\eta \sinh^2 r} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}. \quad (\text{C5})$$

This implies that $\mathbf{P}(\mathcal{Q}, \mathbf{v}_{\text{avg}}) = 1$. In the case where there are no losses $\eta = 1$ and $\mathcal{Q} \propto \sinh^2 2r$ as expected.

1. Optimal measurement

We now show that the optimal measurement for estimating the average phase $\theta_{\text{avg}} := (\theta_1 + \theta_2)/2$ in our

two-mode setup is a Gaussian measurement—specifically, an adaptive scheme in which the two-mode squeezed state, after local phase encoding, is passed through a 50:50 beam splitter, followed by homodyne detection at an optimal angle ϕ_{opt} . We begin with the state after the phase shifts, whose covariance matrix is given by Eq. (C2). The two encoded modes are interfered on a single balanced 50: 50 beam splitter. This transformation renders the output state's covariance matrix block-diagonal:

$$\sigma_{\theta, \text{bs}} = \frac{1}{2} \begin{pmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{0} & \mathbf{B} \end{pmatrix} \quad (\text{C6})$$

where $\mathbf{A}$ and $\mathbf{B}$ are matrices given by

$$\mathbf{A} = \frac{1}{2} \begin{pmatrix} 1 - \eta(2\sinh^2 r - \sinh 2r \cos \theta) & -\eta \sinh 2r \sin \theta \\ -\eta \sinh 2r \sin \theta & 1 + \eta(2\sinh^2 r + \sinh 2r \cos \theta) \end{pmatrix} \quad (\text{C7})$$

$$\mathbf{B} = \frac{1}{2} \begin{pmatrix} 1 - \eta(2\sinh^2 r + \sinh 2r \cos \theta) & \eta \sinh 2r \sin \theta \\ \eta \sinh 2r \sin \theta & 1 - \eta(\sinh 2r \cos \theta - 2\sinh^2 r) \end{pmatrix}. \quad (\text{C8})$$

The symmetry and block-diagonal form of the covariance matrix allows us to analyze each output port independently, simplifying the analysis of measurement strategies. We now turn to the measurement stage, where homodyne detection is performed on each output port of the beam splitter. Port 1 is measured in a rotated $\hat{x}_\phi$ quadrature, while port 2 is measured in the conjugate $\hat{p}_\phi$ quadrature. Specifically, the measurement covariance matrices are taken in the limiting form:

$$\begin{aligned} \sigma_{\text{M}}^{(1)} &= R(\phi) \text{diag} \left(\frac{1}{r_1}, r_1 \right) R(\phi)^\top \quad \text{and} \\ \sigma_{\text{M}}^{(2)} &= R(\phi) \text{diag} \left(r_2, \frac{1}{r_2} \right) R(\phi)^\top \end{aligned} \quad (\text{C9})$$

where $R(\phi)$ is a rotation matrix with r_1 and r_2 being squeezing parameters. In the limit $r_1 \rightarrow \infty$ and $r_2 \rightarrow \infty$,

these measurements become projective: Party 1 effectively measures $\hat{x}_\phi$, and party 2, $\hat{p}_\phi$, with infinite precision along those directions and maximal uncertainty in their conjugates.

The classical Fisher information can be expressed in terms of the first and second moments as follows [51]

$$\begin{aligned} \mathcal{F}_C(\theta; \mathbf{r}_\theta, \sigma_\theta; \sigma_{\text{M}}) &= \frac{1}{2} \text{tr} \left[(\sigma_\theta + \sigma_{\text{M}})^{-1} \left(\frac{\partial \sigma_\theta}{\partial \theta} \right) \right]^2 \\ &\quad + \left(\frac{\partial \mathbf{r}_\theta}{\partial \theta} \right)^\top (\sigma_\theta + \sigma_{\text{M}})^{-1} \left(\frac{\partial \mathbf{r}_\theta}{\partial \theta} \right). \end{aligned} \quad (\text{C10})$$

The optimal measurement angle is obtained by maximizing $\mathcal{F}_C(\phi)$ with respect to ϕ . This yields:

$$\phi_{\text{opt}} = \frac{\theta_1 + \theta_2}{2} + \tan^{-1} \left(\frac{\eta \sinh 2r}{\sqrt{1 + 4(1 - \eta)\eta \sinh^2 r}} \right). \quad (\text{C11})$$

Finally, plugging ϕ_{opt} into the classical FI yields:

$$\mathcal{F}_c(r) = \frac{2\eta^2 \sinh^2 2r}{1 + 4(1 - \eta)\eta \sinh^2 r}. \quad (\text{C12})$$

APPENDIX D: COVARIANCES AND QUANTUM FISHER INFORMATION MATRIX OF A TWO-MODE SQUEEZED STATE THROUGH A BALANCED TREE

In this appendix we derive closed-form expressions for the covariance matrix of a state that starts as a two-mode squeezed state and is then split into $M = 2^N$ modes ($N \geq 2$) by a balanced beam splitter tree. At each layer, every mode is mixed on a 50:50 beam splitter with vacuum in the ancillary port (see Fig. 8). We then give the covariance matrix after 2^N local phase shifts are encoded on the modes. Finally, we obtain an analytical form of the quantum Fisher information matrix, together with its eigenvalues and eigenvectors. The entire appendix can also be reproduced using a *Mathematica* notebook (see Ref. [47]), where all matrices are provided and the results can be verified both analytically and numerically. For clarity, the discussion is organized into three parts.

1. Compact expression for the beam-splitter tree covariance matrix

In this subsection we derive compact formulas for the “leaf-to-leaf” covariances $\sigma_{jk}^{(x)}$ and $\sigma_{jk}^{(p)}$ generated by a balanced beam-splitter tree fed by a two-mode squeezed

state on inputs A, B . The key idea is that each output quadrature $\hat{z}_j$ can be written as a scaled version of one of the original input quadratures (A or B) together with extra terms coming from the vacuum modes that enter the unused ports of the beam splitters. These extra terms have simple $\pm$ signs that depend on the path through the tree. We will keep track of these signs and scaling factors, compute the covariances coming from the squeezed inputs and the vacua separately, then add them to obtain explicit formulas for $\sigma_{jk}^{(x)}$ and $\sigma_{jk}^{(p)}$. Finally, we combine them into the global block-diagonal covariance matrix $\sigma = \sigma^{(x)} \oplus \sigma^{(p)}$.

For a mode m mixed with an ancillary vacuum mode v , a balanced beam splitter acts on the dimensionless quadratures

$$\begin{pmatrix} x_m \\ x_v \end{pmatrix} \rightarrow \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} x_m \\ x_v \end{pmatrix}, \quad (\text{D1})$$

$$\begin{pmatrix} p_m \\ p_v \end{pmatrix} \rightarrow \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} p_m \\ p_v \end{pmatrix}.$$

Because (D1) is block-diagonal in (x, p) , it creates no cross x - p correlations provided the input state itself is free of such terms. We adopt this assumption throughout.

Let A and B denote the two modes that carry an initial two-mode squeezed state; every remaining input port is prepared in vacuum. A balanced binary tree of 50:50 beam splitters of depth N doubles the mode count at each layer. We count layers starting from 1; hence a tree of depth N contains $N - 1$ beam-splitter layers and produces $M = 2^N$ output modes (see Fig. 8).

We label leaves and layers by $j \in \{0, 1, \dots, 2^N - 1\}$ and $\ell \in \{1, \dots, N - 1\}$, and set

$$j_i(j) := \lfloor j/2^i \rfloor \bmod 2 \quad (i \in \mathbb{N}_0), \quad (\text{D2})$$

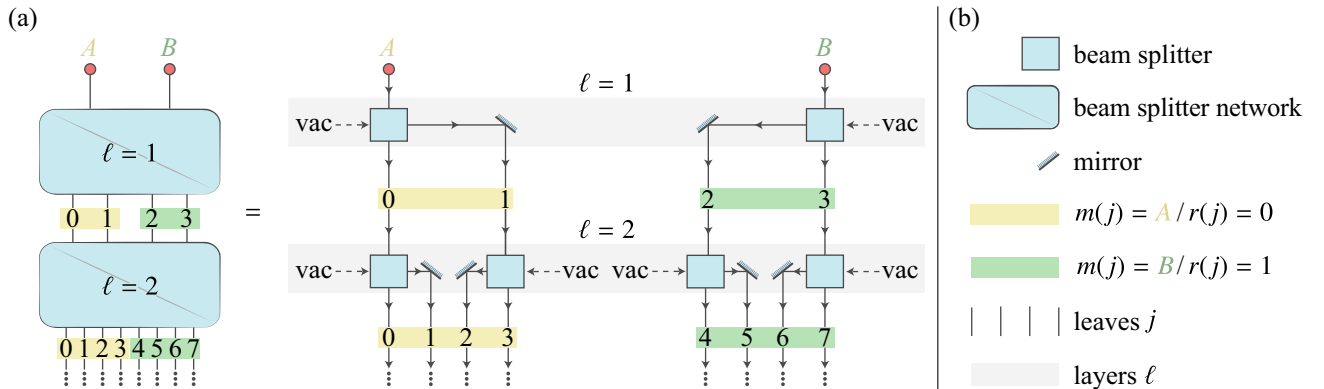


FIG. 8. Beam-splitter tree. (a) A two-mode squeezed state (A, B) is split into $M = 2^N$ modes ($N \geq 2$) by a balanced beam-splitter tree. At each layer ℓ , every mode is mixed on a 50:50 beam splitter with vacuum in the ancillary port. The leaves j at the output originate either from A or B ; we indicate the origin by coloring the leaves in yellow ($m(j) = A/r(j) = 0$) or green ($m(j) = B/r(j) = 1$). Leaf indices j and layer indices ℓ follow the conventions defined in Eqs. (D2) and (D6). (b) Legend showing the optical elements used in the beam-splitter tree.

$$r(j) := j_{N-1}(j), \quad (\text{D3})$$

$$s_\ell(j) := (-1)^{j_{N-\ell-1}(j)}, \quad (\text{D4})$$

$$b(j, \ell) := \lfloor j/2^{N-\ell} \rfloor. \quad (\text{D5})$$

The following lemma gives an explicit expression for the quadrature operator at each output mode in terms of the initial inputs and the vacuum contributions introduced at each layer of the beam splitter tree:

Lemma 9. For any $z \in \{x, p\}$ and every leaf j ,

$$\hat{z}_j = 2^{-(N-1)/2} \hat{z}_{m(j)} + \sum_{\ell=1}^{N-1} 2^{-(N-\ell)/2} s_\ell(j) \hat{z}_{\text{vac}}^{(\ell, b(j, \ell))}, \quad (\text{D6})$$

where $m(j) = A$ if $r(j) = 0$ and $m(j) = B$ if $r(j) = 1$.

Proof. The proof proceeds by induction on the network depth N . For the base case $N = 2$, the tree contains two beam splitters, each mixing one of A, B with a fresh vacuum. Applying (D1) once gives

$$\hat{z}_j = 2^{-1/2} \hat{z}_{m(j)} + 2^{-1/2} s_1(j) \hat{z}_{\text{vac}}^{(1, b(j, 1))}, \quad (\text{D7})$$

which matches (D6) for $N = 2$. Assume (D6) holds for depth $N - 1$. Attach to every leaf a balanced beam splitter that mixes the leaf with a fresh vacuum $\hat{z}_{\text{vac}}^{(N-1, b)}$ ($b = 0, \dots, 2^{N-1} - 1$). Denote by $\hat{z}_j^{(\text{old})}$ the quadrature on the depth- $(N - 1)$ leaf j before the extra splitter is inserted. The two new leaves, labelled $2j$ and $2j + 1$, obey

$$\hat{z}_{2j+\nu} = 2^{-1/2} \left[\hat{z}_j^{(\text{old})} + (-1)^\nu \hat{z}_{\text{vac}}^{(N-1, b)} \right] \quad \text{for } \nu \in \{0, 1\}. \quad (\text{D8})$$

Inserting the induction hypothesis for $\hat{z}_j^{(\text{old})}$ and observing that $(-1)^\nu = s_{N-1}(2j + \nu)$ yields (D6) for depth N . The identities $b(2j + \nu, \ell) = b(j, \ell)$ and $s_\ell(2j + \nu) = s_\ell(j)$ for $\ell < N - 1$ follow directly from the definitions, completing the proof. ■

Next, we use the previous lemma to decompose each output quadrature into its squeezed and vacuum contributions, in preparation for computing covariances between the leaf modes. Define

$$\begin{aligned} \hat{z}_j^{(\text{sq})} &:= 2^{-(N-1)/2} \hat{z}_{m(j)} \quad \text{and} \\ \hat{z}_j^{(\text{vac})} &:= \sum_{\ell=1}^{N-1} 2^{-(N-\ell)/2} s_\ell(j) \hat{z}_{\text{vac}}^{(\ell, b(j, \ell))}. \end{aligned} \quad (\text{D9})$$

Because the initial TMSS pair (A, B) and all ancilla vacua are uncorrelated and the network is a real orthogonal (hence symplectic) transformation on (x, p) , cross terms

remain zero: $\langle \hat{z}_j^{(\text{sq})} \hat{z}_k^{(\text{vac})} \rangle = 0$ for all j, k . With $\hat{x} = (\hat{a} + \hat{a}^\dagger)/\sqrt{2}$ and $\hat{p} = (\hat{a} - \hat{a}^\dagger)/(i\sqrt{2})$, the TMSS state satisfies $\text{cov}(\hat{x}_A, \hat{x}_B) = -\frac{1}{2} \sinh 2r$ and $\text{cov}(\hat{p}_A, \hat{p}_B) = \frac{1}{2} \sinh 2r$. Propagating through the tree gives

$$\begin{aligned} \text{cov}(\hat{x}_j^{(\text{sq})}, \hat{x}_k^{(\text{sq})}) &= \frac{1}{2^N} [\cosh 2r \delta_{m(j), m(k)} \\ &\quad - \sinh 2r (1 - \delta_{m(j), m(k)})], \end{aligned} \quad (\text{D10})$$

$$\begin{aligned} \text{cov}(\hat{p}_j^{(\text{sq})}, \hat{p}_k^{(\text{sq})}) &= \frac{1}{2^N} [\cosh 2r \delta_{m(j), m(k)} \\ &\quad + \sinh 2r (1 - \delta_{m(j), m(k)})]. \end{aligned} \quad (\text{D11})$$

For the vacuum ancillas, we have $\langle \hat{z}_{\text{vac}}^{(\ell, b)} \hat{z}_{\text{vac}}^{(\ell', b')} \rangle = \frac{1}{2} \delta_{\ell, \ell'} \delta_{b, b'}$, so

$$\text{cov}(\hat{z}_j^{(\text{vac})}, \hat{z}_k^{(\text{vac})}) = \frac{1}{2} \sum_{\ell=1}^{N-1} 2^{-(N-\ell)} s_\ell(j) s_\ell(k) \delta_{b(j, \ell), b(k, \ell)}. \quad (\text{D12})$$

Adding (D10)–(D12) yields

$$\begin{aligned} \sigma_{jk}^{(x)} &= 2^{-N} [\cosh 2r \delta_{m(j), m(k)} - \sinh 2r (1 - \delta_{m(j), m(k)})] \\ &\quad + \frac{1}{2} \sum_{\ell=1}^{N-1} 2^{-(N-\ell)} s_\ell(j) s_\ell(k) \delta_{b(j, \ell), b(k, \ell)}, \end{aligned} \quad (\text{D13})$$

$$\begin{aligned} \sigma_{jk}^{(p)} &= 2^{-N} [\cosh 2r \delta_{m(j), m(k)} + \sinh 2r (1 - \delta_{m(j), m(k)})] \\ &\quad + \frac{1}{2} \sum_{\ell=1}^{N-1} 2^{-(N-\ell)} s_\ell(j) s_\ell(k) \delta_{b(j, \ell), b(k, \ell)}, \end{aligned} \quad (\text{D14})$$

which are symmetric and positive-definite. Now we collect the x - and p -covariances into the full $2M \times 2M$ covariance matrix. Because the $\hat{x}$ and $\hat{p}$ quadratures remain uncorrelated throughout the network, the global covariance matrix takes the block-diagonal form

$$\sigma = \sigma^{(x)} \oplus \sigma^{(p)}, \quad (\text{D15})$$

with the canonical ordering $(\hat{x}_0, \hat{x}_1, \dots, \hat{x}_{M-1}, \hat{p}_0, \hat{p}_1, \dots, \hat{p}_{M-1})$. Alternatively, using the interleaved ordering $(\hat{x}_0, \hat{p}_0, \hat{x}_1, \hat{p}_1, \dots)$, we define a permutation $\mathcal{P}$ such that

$$\sigma = \mathcal{P} \begin{pmatrix} \sigma^{(x)} & 0 \\ 0 & \sigma^{(p)} \end{pmatrix} \mathcal{P}^\top, \quad (\text{D16})$$

where $\mathcal{P}(2j) = j$, $\mathcal{P}(2j+1) = M+j$ for $j = 0, \dots, M-1$. This completes the construction of the full covariance matrix of the output state.

2. Covariance matrix phase-shift

In this subsection we describe how the covariance matrix changes when local phase shifts are applied to each output mode of the beam-splitter tree. Each phase shift θ_j acts as a rotation in the (x, p) quadrature space of mode j , and all such rotations together form a block-diagonal symplectic matrix $S(\boldsymbol{\theta})$. By applying the standard transformation rule $\boldsymbol{\sigma} \mapsto S(\boldsymbol{\theta})\boldsymbol{\sigma}S(\boldsymbol{\theta})^\top$ to the block-diagonal covariance from the previous section, we obtain explicit formulas for the rotated covariance blocks $\boldsymbol{\sigma}^{(xx)}(\boldsymbol{\theta})$, $\boldsymbol{\sigma}^{(xp)}(\boldsymbol{\theta})$, $\boldsymbol{\sigma}^{(px)}(\boldsymbol{\theta})$, and $\boldsymbol{\sigma}^{(pp)}(\boldsymbol{\theta})$.

Consider the zero-mean Gaussian state produced by the beam splitter tree of depth N given by Eq. (D15). Let $\boldsymbol{\theta} = (\theta_0, \dots, \theta_{M-1}) \in \mathbb{R}^M$ and define the symplectic matrix:

$$S(\boldsymbol{\theta}) = \bigoplus_{j=0}^{M-1} \begin{pmatrix} \cos \theta_j & \sin \theta_j \\ -\sin \theta_j & \cos \theta_j \end{pmatrix}. \quad (\text{D17})$$

The local phase-rotation unitary $\hat{U}(\boldsymbol{\theta}) = \prod_{j=0}^{M-1} e^{-i\theta_j \hat{a}_j^\dagger \hat{a}_j}$ transforms the covariance matrix as

$$\boldsymbol{\sigma}(\boldsymbol{\theta}) := S(\boldsymbol{\theta})\boldsymbol{\sigma}S(\boldsymbol{\theta})^\top = \begin{pmatrix} \boldsymbol{\sigma}^{(xx)}(\boldsymbol{\theta}) & \boldsymbol{\sigma}^{(xp)}(\boldsymbol{\theta}) \\ \boldsymbol{\sigma}^{(px)}(\boldsymbol{\theta}) & \boldsymbol{\sigma}^{(pp)}(\boldsymbol{\theta}) \end{pmatrix}, \quad (\text{D18})$$

with entries for $j, k = 0, \dots, M-1$,

$$\sigma_{jk}^{(xx)}(\boldsymbol{\theta}) = \cos \theta_j \cos \theta_k \sigma_{jk}^{(x)} + \sin \theta_j \sin \theta_k \sigma_{jk}^{(p)}, \quad (\text{D19})$$

$$\sigma_{jk}^{(xp)}(\boldsymbol{\theta}) = -\cos \theta_j \sin \theta_k \sigma_{jk}^{(x)} + \sin \theta_j \cos \theta_k \sigma_{jk}^{(p)}, \quad (\text{D20})$$

$$\sigma_{jk}^{(px)}(\boldsymbol{\theta}) = -\sin \theta_j \cos \theta_k \sigma_{jk}^{(x)} + \sin \theta_j \sin \theta_k \sigma_{jk}^{(p)}, \quad (\text{D21})$$

$$\sigma_{jk}^{(pp)}(\boldsymbol{\theta}) = \sin \theta_j \sin \theta_k \sigma_{jk}^{(x)} + \cos \theta_j \cos \theta_k \sigma_{jk}^{(p)}. \quad (\text{D22})$$

The form of Eq. (D18) is easily understood once one recalls how a phase-rotation acts in the Heisenberg picture. First, for each mode j ,

$$\hat{U}(\boldsymbol{\theta})^\dagger \begin{pmatrix} \hat{x}_j \\ \hat{p}_j \end{pmatrix} U(\boldsymbol{\theta}) = \begin{pmatrix} \cos \theta_j & \sin \theta_j \\ -\sin \theta_j & \cos \theta_j \end{pmatrix} \begin{pmatrix} \hat{x}_j \\ \hat{p}_j \end{pmatrix}. \quad (\text{D23})$$

Because a linear (and, in particular, symplectic) transformation S carries the covariance matrix to $\boldsymbol{\sigma} \mapsto S(\boldsymbol{\theta})\boldsymbol{\sigma}S(\boldsymbol{\theta})^\top$, the full transformation law follows at once. Finally, substituting the block-diagonal form of the original $\boldsymbol{\sigma}$ and the block structure of $S(\boldsymbol{\theta})$ yields the explicit block expression displayed in Eq. (D18).

3. Quantum Fisher information from a beam splitter tree

We now compute the quantum Fisher information matrix for estimating the local phases $\boldsymbol{\theta}$ applied to the modes at the output of the beam-splitter tree and determine its eigenvalues and eigenvectors in closed form. Starting from the covariances $\sigma_{jk}^{(x)}$ and $\sigma_{jk}^{(p)}$ derived earlier, we first show that the QFI does not depend on the actual phase values, so it can be evaluated at $\boldsymbol{\theta} = \mathbf{0}$. We then use the symmetry of the tree to prove that $\mathbf{Q}$ has only three distinct kinds of entries, which allows us to write it in a simple projector form. This structure makes the eigendecomposition straightforward: two special phase patterns ($\mathbf{u}_+$ for a uniform phase and $\mathbf{u}_0$ for an A vs B imbalance) give two of the eigenvalues, and any vector orthogonal to both lies in a degenerate subspace with a common eigenvalue $\lambda_\perp$.

Consider the zero-mean Gaussian output of the depth- N beam-splitter tree fed by a two-mode squeezed state on inputs A, B (all other inputs in vacuum), with quadrature covariances $\sigma_{jk}^{(x)}, \sigma_{jk}^{(p)}$ given by Eqs. (D13) and (D14). Below, we prove that after encoding local phase shifts as in Eq. (D18), the QFI $\mathbf{Q}$:

(a) is independent of $\boldsymbol{\theta}$ and has entries

$$Q_{jk} = 2[(\sigma_{jk}^{(x)})^2 + (\sigma_{jk}^{(p)})^2] - \delta_{jk}; \quad (\text{D24})$$

(b) admits the projector form

$$\mathbf{Q} = \lambda_\perp (\mathbb{1}_M - \Pi_+ - \Pi_0) + \lambda_+ \Pi_+ \quad \text{with} \\ \Pi_+ := \frac{\mathbf{1}\mathbf{1}^\top}{M} \quad \text{and} \quad \Pi_0 := \frac{\mathbf{s}\mathbf{s}^\top}{M}, \quad (\text{D25})$$

where $\mathbf{1} = (1, \dots, 1)^\top$ and $\mathbf{s} = (\underbrace{1, \dots, 1}_{\frac{M}{2}}, \underbrace{-1, \dots, -1}_{\frac{M}{2}})^\top$;

(c) has spectrum

$$\lambda(\mathbf{Q}) = \left\{ 0, \underbrace{\frac{\cosh 2r - 1}{2^{N-2}}, \dots, \frac{\cosh 2r - 1}{2^{N-2}}}_{M-2 \text{ times}}, \frac{\cosh 4r - 1}{2^{N-1}} \right\}. \quad (\text{D26})$$

Equivalently, entrywise,

$$Q_{jk} = \begin{cases} \lambda_\perp + \frac{\lambda_+ - 2\lambda_\perp}{M}, & j = k, \\ \frac{\lambda_+ - 2\lambda_\perp}{M}, & j \neq k \quad \text{and} \quad m(j) = m(k), \\ \frac{\lambda_+}{M}, & m(j) \neq m(k), \end{cases} \quad (\text{D27})$$

where

$$\lambda_{\perp} = \frac{\cosh 2r - 1}{2^{N-2}} \quad \text{and} \quad \lambda_{+} = \frac{\cosh 4r - 1}{2^{N-1}}. \quad (\text{D28})$$

Step 1 (Independence of θ and entrywise formula). By Lemma 2 and zero mean, the QFI is

$$Q_{jk}(\theta) = 2 \sum_{z,w \in \{x,p\}} \sigma_{z_j \hat{w}_k}(\theta)^2 - \delta_{jk}, \quad (\text{D29})$$

where $\sigma_{z_j \hat{w}_k}(\theta)$ are the second moments after encoding. Using Frobenius-norm invariance under left/right orthogonal multiplications [52],

$$\begin{aligned} \sum_{z,w} \sigma_{z_j \hat{w}_k}(\theta)^2 &= \|\sigma_{jk}(\theta)\|_F^2 = \|R(\theta_j) \sigma_{jk}(\mathbf{0}) R(\theta_k)^\top\|_F^2 \\ &= \|\sigma_{jk}(\mathbf{0})\|_F^2 = (\sigma_{jk}^{(x)})^2 + (\sigma_{jk}^{(p)})^2. \end{aligned} \quad (\text{D30})$$

Thus $Q_{jk}(\theta)$ is independent of θ , and evaluating at $\theta = \mathbf{0}$ yields (D24).

Step 2 (Projector form and commutant). Let v_{jk} denote the vacuum contribution appearing in (D13) and (D14):

$$v_{jk} := \frac{1}{2} \sum_{\ell=1}^{N-1} 2^{-(N-\ell)} s_{\ell}(j) s_{\ell}(k) \delta_{b(j,\ell), b(k,\ell)}. \quad (\text{D31})$$

We claim that

$$v_{jk} = \begin{cases} \frac{1}{2}(1 - 2^{1-N}), & j = k, \\ -2^{-N}, & j \neq k \text{ and } m(j) = m(k), \\ 0, & m(j) \neq m(k). \end{cases} \quad (\text{D32})$$

For $j = k$, the signs coincide $s_{\ell}(j) = s_{\ell}(k)$ and all Kronecker deltas are 1, so $v_{jj} = \frac{1}{2} \sum_{\ell=1}^{N-1} 2^{-(N-\ell)} = \frac{1}{2}(1 - 2^{1-N})$. If $m(j) \neq m(k)$, then j and k lie on opposite outputs of the first (top) beam splitter, so $b(j, 1) \neq b(k, 1)$. At every subsequent level $\ell \geq 2$, each side is split further without mixing with the other, hence $b(j, \ell) \neq b(k, \ell)$ for all ℓ . Therefore $\delta_{b(j,\ell), b(k,\ell)} = 0$ for every ℓ , and $v_{jk} = 0$. Now take $j \neq k$ with $m(j) = m(k)$. Let $L \in \{2, \dots, N-1\}$ be the smallest level at which j and k choose different outputs (equivalently, the last level where they coincide is $L-1$). Then only the terms with $\ell = 1, \dots, L-1$ contribute to v_{jk} . For $\ell \leq L-2$ their choices agree, so $s_{\ell}(j) s_{\ell}(k) = +1$, whereas at $\ell = L-1$ they differ and $s_{L-1}(j) s_{L-1}(k) = -1$. Hence,

$$\begin{aligned} v_{jk} &= \frac{1}{2} \left[\sum_{\ell=1}^{L-2} 2^{-(N-\ell)} - 2^{-(N-L+1)} \right] \\ &= \frac{1}{2} [2^{-(N-L+1)} (1 - 2^{-(L-2)}) - 2^{-(N-L+1)}] = -2^{-N}, \end{aligned} \quad (\text{D33})$$

proving Eq. (D32).

According to Eq. (D32) and the structure of the squeezed part in (D13) and (D14), the entries of Q_{jk} in (D24) take only three values: one for $j = k$, one for $j \neq k$ with $m(j) = m(k)$, and one for $m(j) \neq m(k)$. Hence Q is completely determined by three numbers and can be written as

$$Q = \alpha \mathbb{1}_M + \beta \Pi_{+} + \gamma \Pi_0, \quad (\text{D34})$$

for some scalars α, β, γ , where $\Pi_{+} = \mathbf{1}\mathbf{1}^\top / M$ and $\Pi_0 = ss^\top / M$, with

$$\begin{aligned} \mathbf{1}\mathbf{1}^\top &= \begin{pmatrix} \mathbf{1}_A \mathbf{1}_A^\top & \mathbf{1}_A \mathbf{1}_B^\top \\ \mathbf{1}_B \mathbf{1}_A^\top & \mathbf{1}_B \mathbf{1}_B^\top \end{pmatrix} \quad \text{and} \\ ss^\top &= \begin{pmatrix} \mathbf{1}_A \mathbf{1}_A^\top & -\mathbf{1}_A \mathbf{1}_B^\top \\ -\mathbf{1}_B \mathbf{1}_A^\top & \mathbf{1}_B \mathbf{1}_B^\top \end{pmatrix}. \end{aligned} \quad (\text{D35})$$

where $\mathbf{1}_A$ and $\mathbf{1}_B$ denote the all-ones vectors of length $\frac{M}{2}$ on the A and B indices, respectively.

Step 3 (Eigenspaces and eigenvalues). We now pick two phase patterns that match the symmetry of the tree and make the QFI simple to evaluate. If we vary the phases along a unit vector $\mathbf{u} \in \mathbb{R}^M$ via $\theta = t\mathbf{u}$, the unitary is $\hat{U}(t) = \exp(-it \hat{G}_u)$ with generator

$$\hat{G}_u := \sum_{j=0}^{M-1} u_j \hat{n}_j. \quad (\text{D36})$$

For our zero-mean Gaussian setting, one has $\mathbf{u}^\top Q \mathbf{u} = 4 \text{var}(\hat{G}_u)$, so we want directions $\mathbf{u}$ for which $\hat{G}_u$ has a simple form on our state. Define,

$$\begin{aligned} \mathbf{u}_{+} &= \frac{\mathbf{1}}{\sqrt{M}} \quad \text{and} \quad \mathbf{u}_0 = \frac{\mathbf{s}}{\sqrt{M}}, \quad \text{where} \\ s_j &= \begin{cases} +1, & j \in A \\ -1, & j \in B. \end{cases} \end{aligned} \quad (\text{D37})$$

These correspond to a uniform phase (all modes together) and an A -vs- B imbalance (plus on A , minus on B). A passive beam-splitter network redistributes photons but does not create or destroy them. Since all ancillary inputs (other than A, B) are in vacuum, the total photon number flowing down the A -branch equals the photon number that entered at A , and similarly for B :

$$\sum_{j \in A} \hat{n}_j = \hat{n}_A, \quad \sum_{k \in B} \hat{n}_k = \hat{n}_B, \quad \sum_{j=0}^{M-1} \hat{n}_j = \hat{n}_A + \hat{n}_B. \quad (\text{D38})$$

Consequently, the generators for $\mathbf{u}_+$ and $\mathbf{u}_0$ collapse to

$$\begin{aligned} \hat{G}_+ &= \sum_j \frac{1}{\sqrt{M}} \hat{n}_j = \frac{\hat{n}_A + \hat{n}_B}{\sqrt{M}}, \\ \hat{G}_0 &= \sum_j \frac{s_j}{\sqrt{M}} \hat{n}_j = \frac{\hat{n}_A - \hat{n}_B}{\sqrt{M}}. \end{aligned} \quad (\text{D39})$$

These simple number combinations make the corresponding variances, and hence the eigenvalues of $\mathbf{Q}$ along $\mathbf{u}_+$ and $\mathbf{u}_0$, straightforward to compute for a TMSS. For a TMSS with squeezing r and $\bar{n} := \sinh^2 r$, $\text{var}(\hat{n}_A) = \text{var}(\hat{n}_B) = \bar{n}(\bar{n} + 1)$, $\text{cov}(\hat{n}_A, \hat{n}_B) = \bar{n}(\bar{n} + 1)$, so $\text{var}(\hat{n}_A + \hat{n}_B) = 4\bar{n}(\bar{n} + 1)$ and $\text{var}(\hat{n}_A - \hat{n}_B) = 0$. For our pure state under local phase shifts, the QFI satisfies along any direction $\mathbf{u}$: $\mathbf{u}^\top \mathbf{Q} \mathbf{u} = 4 \text{var}(\hat{G}_u)$. Since $\mathbf{u}_+$ and $\mathbf{u}_0$ are normalized and are eigenvectors by symmetry, their eigenvalues are $\lambda_\pm = 4 \text{var}(\hat{G}_\pm)$. Computing then, we have that for $\mathbf{u}_+$:

$$\text{var}(\hat{G}_+) = \frac{1}{M} \text{var}(\hat{n}_A + \hat{n}_B) = \frac{4\bar{n}(\bar{n} + 1)}{M} = \frac{\cosh 4r - 1}{2^{N-1}}. \quad (\text{D40})$$

For $\mathbf{u}_0$, it follows that

$$\text{var}(\hat{G}_0) = \frac{1}{M} \text{var}(\hat{n}_A - \hat{n}_B) = 0. \quad (\text{D41})$$

Finally, from the three-valued structure of $\mathbf{Q}_{jk}$, the QFI lies in the three-dimensional linear span generated by $\{\mathbf{1}, \Pi_+, \Pi_0\}$. Consequently, $\mathbb{R}^M$ decomposes into three invariant (mutually orthogonal) subspaces: $\text{span}\{\mathbf{u}_+\} \oplus \text{span}\{\mathbf{u}_0\} \oplus \mathcal{W}$, where $\mathcal{W} := \{\mathbf{w} : \mathbf{1}^\top \mathbf{w} = 0, \mathbf{s}^\top \mathbf{w} = 0\}$. On $\mathcal{W}$, we have $\Pi_+ \mathbf{w} = \Pi_0 \mathbf{w} = 0$. So, $\mathbf{Q} \mathbf{w} = \lambda_\perp \mathbf{w}$. To obtain the eigenvalue, choose $\mathbf{w}$ supported on two sibling leaves j, k in the same half created by the last balanced splitter, with entries $w_j = 1, w_k = -1$, others 0. The associated generator is $\hat{G}_\perp = \frac{\hat{n}_j - \hat{n}_k}{\sqrt{2}}$. Writing the last splitter as $\hat{a}_j = \frac{1}{\sqrt{2}}(\hat{c} + \hat{v})$, $\hat{a}_k = \frac{1}{\sqrt{2}}(\hat{c} - \hat{v})$ with $\hat{v}$ a fresh vacuum and $\hat{c}$ the parent mode one layer above, one finds $\hat{n}_j - \hat{n}_k = \hat{c}^\dagger \hat{v} + \hat{v}^\dagger \hat{c}$. On a product state $\rho_c \otimes |0\rangle\langle 0|_v$ (i.e. $\hat{v}$ in vacuum and uncorrelated with $\hat{c}$),

$$\text{var}(\hat{n}_j - \hat{n}_k) = \langle (\hat{c}^\dagger \hat{v} + \hat{v}^\dagger \hat{c})^2 \rangle = \langle \hat{c}^\dagger \hat{c} \rangle, \quad (\text{D42})$$

since $\langle \hat{v}^\dagger \hat{v} \rangle = 0$, $\langle \hat{v} \hat{v}^\dagger \rangle = 1$ and all mixed expectations factorize. Therefore

$$\lambda_\perp = \frac{\mathbf{w}^\top \mathbf{Q} \mathbf{w}}{\|\mathbf{w}\|^2} = 4 \text{var}(\hat{G}_\perp) = 2 \text{var}(\hat{n}_j - \hat{n}_k) \stackrel{(\text{D43})}{=} 2 \langle \hat{c}^\dagger \hat{c} \rangle. \quad (\text{D43})$$

Each 50:50 splitter with vacuum halves the mean photon number on the transmitted branch: if $\hat{a}_{\text{out}} = (\hat{a}_{\text{in}} + \hat{v})/\sqrt{2}$ with $\hat{v}$ in vacuum then $\langle \hat{a}_{\text{out}}^\dagger \hat{a}_{\text{out}} \rangle = \frac{1}{2} \langle \hat{a}_{\text{in}}^\dagger \hat{a}_{\text{in}} \rangle$. Along any path from an input to a leaf there are $N - 1$ splitters; consequently the leaf mean is $\bar{n}/2^{N-1}$. The parent mode $\hat{c}$ sits one layer above the leaves, so it has passed through $N - 2$ splitters and $\langle \hat{c}^\dagger \hat{c} \rangle = \frac{\bar{n}}{2^{N-2}}$. Substituting into (D43) and recalling $\cosh 2r - 1 = 2\bar{n}$ gives

$$\lambda_\perp = \frac{2\bar{n}}{2^{N-2}} = \frac{\cosh 2r - 1}{2^{N-2}} \quad (\text{D44})$$

Therefore $\mathbf{Q}$ has eigenvalue 0 on $\text{span}\{\mathbf{u}_0\}$, eigenvalue λ_+ on $\text{span}\{\mathbf{u}_+\}$, and eigenvalue $\lambda_\perp$ on $\mathcal{W}$, which is equivalent to the projector form (D25) and to the spectrum (D26). The casewise expression (D27) follows from (D25) by evaluating the three cases $j = k$, $j \neq k$ with $m(j) = m(k)$, and $m(j) \neq m(k)$.

4. Average number of photons hitting the phase-shift

In the previous appendix, we proved that the eigenvalues of the QFI associated with the 2^N -mode Gaussian state generated by recursively distributing a two-mode squeezed vacuum through a balanced beam splitter network exhibit a highly structured eigenspectrum. More precisely, these are given by

$$\lambda(\mathbf{Q}) = \left\{ 0, \underbrace{\frac{\cosh 2r - 1}{2^{N-2}}, \dots, \frac{\cosh 2r - 1}{2^{N-2}}}_{2^N - 2 \text{ times}}, \frac{\cosh 4r - 1}{2^{N-1}} \right\}. \quad (\text{D45})$$

We now recast them in terms of the mean photon number. The mean photon number per input mode is $\bar{n} := \sinh^2 r$, so the total mean photon number on the two-mode squeezed state is $\bar{N} := 2 \sinh^2 r$. After the balanced 2^N -port splitter network, this total is conserved and spread uniformly, hence the mean photons per output mode (i.e., per local phase parameter) is

$$\bar{n}_{\text{mode}} = \frac{\bar{N}}{2^N} = 2^{1-N} \sinh^2 r. \quad (\text{D46})$$

Using the identities $\cosh 2r - 1 = 2 \sinh^2 r$ and $\cosh 4r - 1 = 2 \sinh^2 2r = 8 \sinh^2 r \cosh^2 r$, the spectrum can be written as

$$\lambda(\mathbf{Q}) = \left\{ 0, \underbrace{4\bar{n}_{\text{mode}}, \dots, 4\bar{n}_{\text{mode}}}_{2^N - 2 \text{ times}}, 8\bar{n}_{\text{mode}}(1 + 2^{N-1}\bar{n}_{\text{mode}}) \right\}. \quad (\text{D47})$$

For fixed N , the QFI spectrum splits into three sectors: one null direction, a $(2^N - 2)$ -dimensional shot-noise sector with eigenvalues $\lambda_{\text{SNL}} := 4\bar{n}_{\text{mode}}$ that grow linearly with the mean photons per mode, and one enhanced direction with $\lambda_{\text{max}} := 8\bar{n}_{\text{mode}}(1 + 2^{N-1}\bar{n}_{\text{mode}})$ that includes a quadratic term from squeezing-induced correlations. In terms of total photons $\bar{N} = 2^N \bar{n}_{\text{mode}}$, these become $\lambda_{\text{SNL}} = \bar{N}/2^{N-2}$ and $\lambda_{\text{max}} = \bar{N}^2/2^{N-2} + 8\bar{N}/2^N$, so the enhancement factor is $\lambda_{\text{max}}/\lambda_{\text{SNL}} = \bar{N} + 2$. Consequently, estimation variances scale as $1/\lambda$: generic phase combinations are

shot-noise limited $\sim 1/\bar{N}$, while the special collective phase achieves Heisenberg scaling $\sim 1/\bar{N}^2$. The factor 2^N only fixes prefactors for a given N —it does not change the photon-number scaling exponent.

APPENDIX E: QUANTUM FISHER INFORMATION MATRIX & PRIVACY

In this appendix, we prove Lemma 2 and Theorem 3. We begin by considering a pure state $|\psi_0\rangle$ and recalling that a local phase shift on mode μ is implemented by the unitary $U(\theta_\mu) = e^{i\theta_\mu \hat{n}_\mu}$, where $\hat{n}_\mu := \hat{a}_\mu^\dagger \hat{a}_\mu$ is the number operator. For pure states, the quantum Fisher information matrix (QFI) is given by

$$\mathbf{Q}_{\mu\nu}(\boldsymbol{\theta}) = 4\text{Re}[\langle \partial_{\theta_\mu} \Psi(\boldsymbol{\theta}) | \partial_{\theta_\nu} \Psi(\boldsymbol{\theta}) \rangle - \langle \partial_{\theta_\mu} \Psi(\boldsymbol{\theta}) | \Psi(\boldsymbol{\theta}) \rangle \langle \Psi(\boldsymbol{\theta}) | \partial_{\theta_\nu} \Psi(\boldsymbol{\theta}) \rangle] \quad (\text{E1})$$

Since the local phase-shift unitaries acting on different modes commute, the derivative with respect to each θ_μ simplifies to:

$$|\partial_{\theta_\mu} \Psi(\boldsymbol{\theta})\rangle = \frac{\partial}{\partial \theta_\mu} (e^{i\theta_\mu \hat{n}_\mu} |\psi_0\rangle) = i\hat{n}_\mu |\Psi(\boldsymbol{\theta})\rangle. \quad (\text{E2})$$

Plugging Eq. (E2) into Eq. (E1), we find that the QFI is given by the covariance of the number operators μ and ν , i.e.,

$$\mathbf{Q}_{\mu\nu}(\boldsymbol{\theta}) = 4[\langle \hat{n}_\mu \hat{n}_\nu \rangle - \langle \hat{n}_\mu \rangle \langle \hat{n}_\nu \rangle] = 4 \text{cov}(\hat{n}_\mu, \hat{n}_\nu) \quad (\text{E3})$$

where all expectation values $\langle \bullet \rangle = \langle \Psi(\boldsymbol{\theta}) | \bullet | \Psi(\boldsymbol{\theta}) \rangle$ are taken with respect to the final state.

We now show that the covariance of number operators can be computed directly from the covariance matrix of the state. First, we express the number operator in terms of quadratures: $\hat{n}_\mu = \hat{a}_\mu^\dagger \hat{a}_\mu = \frac{1}{2}(\hat{x}_\mu - i\hat{p}_\mu)(\hat{x}_\mu + i\hat{p}_\mu) = \frac{1}{2}(\hat{x}_\mu^2 + \hat{p}_\mu^2 - 1)$, where $\hat{a} = (\hat{x}_\mu + i\hat{p}_\mu)/\sqrt{2}$. For zero-mean Gaussian states, all odd moments vanish, and fourth-order moments can be reduced using Wick's theorem [53]

$$\begin{aligned} \langle \hat{z}_\alpha \hat{z}_\beta \hat{z}_\gamma \hat{z}_\delta \rangle &= \langle \hat{z}_\alpha \hat{z}_\beta \rangle \langle \hat{z}_\gamma \hat{z}_\delta \rangle + \langle \hat{z}_\alpha \hat{z}_\gamma \rangle \langle \hat{z}_\beta \hat{z}_\delta \rangle + \langle \hat{z}_\alpha \hat{z}_\delta \rangle \langle \hat{z}_\beta \hat{z}_\gamma \rangle, \\ \langle \hat{z}_\alpha \hat{z}_\beta \hat{w}_\gamma \hat{w}_\delta \rangle &= \langle \hat{z}_\alpha \hat{z}_\beta \rangle \langle \hat{w}_\gamma \hat{w}_\delta \rangle + \langle \hat{z}_\alpha \hat{w}_\gamma \rangle \langle \hat{z}_\beta \hat{w}_\delta \rangle + \langle \hat{z}_\alpha \hat{w}_\delta \rangle \langle \hat{z}_\beta \hat{w}_\gamma \rangle, \end{aligned} \quad (\text{E4})$$

where $\hat{z}, \hat{w} \in \{\hat{x}, \hat{p}\}$. In particular, setting $\alpha = \beta = \mu$ and $\gamma = \delta = \nu$, we obtain:

$$\langle \hat{z}_\mu^2 \hat{z}_\nu^2 \rangle = \langle \hat{z}_\mu^2 \rangle \langle \hat{z}_\nu^2 \rangle + 2\langle \hat{z}_\mu \hat{z}_\nu \rangle^2, \quad (\text{E5})$$

$$\langle \hat{z}_\mu^2 \hat{w}_\nu^2 \rangle = \langle \hat{z}_\mu^2 \rangle \langle \hat{w}_\nu^2 \rangle + 2\langle \hat{z}_\mu \hat{w}_\nu \rangle^2. \quad (\text{E6})$$

Expanding the terms in $4 \text{cov}(\hat{n}_\mu, \hat{n}_\nu)$ in terms of quadratures $\hat{x}_\mu, \hat{p}_\mu$, we find:

$$4\langle \hat{n}_\mu \hat{n}_\nu \rangle = \langle (\hat{x}_\mu^2 + \hat{p}_\mu^2 - 1)(\hat{x}_\nu^2 + \hat{p}_\nu^2 - 1) \rangle = 1 + \langle \hat{x}_\mu^2 \hat{x}_\nu^2 \rangle + \langle \hat{p}_\mu^2 \hat{p}_\nu^2 \rangle + \langle \hat{x}_\mu^2 \hat{p}_\nu^2 \rangle + \langle \hat{p}_\mu^2 \hat{x}_\nu^2 \rangle - 2\langle \hat{p}_\mu^2 \rangle - 2\langle \hat{x}_\mu^2 \rangle. \quad (\text{E7})$$

$$4\langle \hat{n}_\mu \rangle \langle \hat{n}_\nu \rangle = \langle (\hat{x}_\mu^2 + \hat{p}_\mu^2 - 1)(\hat{x}_\nu^2 + \hat{p}_\nu^2 - 1) \rangle = 1 + \langle \hat{x}_\mu^2 \rangle \langle \hat{x}_\nu^2 \rangle + \langle \hat{p}_\mu^2 \rangle \langle \hat{p}_\nu^2 \rangle + 2\langle \hat{x}_\mu^2 \rangle \langle \hat{p}_\nu^2 \rangle - 2\langle \hat{x}_\mu^2 \rangle - 2\langle \hat{p}_\mu^2 \rangle. \quad (\text{E8})$$

For displaced Gaussian states $\hat{z}_\alpha \rightarrow \delta z_\alpha + \langle \hat{z}_\alpha \rangle$ with $\hat{z} \in \{\hat{x}, \hat{p}\}$ and $\alpha \in \{\mu, \nu\}$, we compute the following product:

$$\begin{aligned} \hat{z}_\mu^2 \hat{w}_\nu^2 &= \delta \hat{z}_\mu^2 \delta \hat{w}_\nu^2 + 2\langle \hat{w}_\nu \rangle \delta \hat{z}_\mu^2 \delta \hat{w}_\nu + \langle \hat{w}_\nu \rangle^2 \delta \hat{z}_\mu^2 + 2\langle \hat{z}_\mu \rangle \delta \hat{z}_\mu \delta \hat{w}_\nu^2 + 4\langle \hat{z}_\mu \rangle \langle \hat{w}_\nu \rangle \delta \hat{z}_\mu \delta \hat{w}_\nu + 2\langle \hat{z}_\mu \rangle \langle \hat{w}_\nu \rangle^2 \delta \hat{z}_\mu + \langle \hat{z}_\mu \rangle^2 \delta \hat{w}_\nu^2 \\ &\quad + 2\langle \hat{z}_\mu \rangle^2 \langle \hat{w}_\nu \rangle \delta \hat{w}_\nu + \langle \hat{z}_\mu \rangle^2 \langle \hat{w}_\nu \rangle^2. \end{aligned} \quad (\text{E9})$$

Taking the expectation value and applying Wick's theorem, we see that all odd fluctuation moments vanish, and the fourth-order moments decompose as:

$$\langle \hat{z}_\mu^2 \hat{w}_\nu^2 \rangle = \langle \delta \hat{z}_\mu^2 \rangle \langle \delta \hat{w}_\nu^2 \rangle + 2\langle \delta \hat{z}_\mu \delta \hat{w}_\nu \rangle^2 + \langle \hat{w}_\nu \rangle^2 \langle \delta \hat{z}_\mu^2 \rangle + \langle \hat{z}_\mu \rangle^2 \langle \delta \hat{w}_\nu^2 \rangle + 4\langle \hat{z}_\mu \rangle \langle \hat{w}_\nu \rangle \langle \delta \hat{z}_\mu \delta \hat{w}_\nu \rangle + \langle \hat{z}_\mu \rangle^2 \langle \hat{w}_\nu \rangle^2. \quad (\text{E10})$$

We can now use Eq. (E10) to compute both terms of $4\text{cov}(n_\mu, n_\nu)$. Starting with the first, we find that $4\langle \hat{n}_\mu \hat{n}_\nu \rangle$ is given by:

$$\begin{aligned} 4\langle \hat{n}_\mu \hat{n}_\nu \rangle &= 1 + \langle \delta \hat{x}_\mu^2 \rangle \langle \delta \hat{x}_\nu^2 \rangle + 2\langle \delta \hat{x}_\mu \delta \hat{x}_\nu \rangle^2 + \langle \hat{x}_\nu \rangle^2 \langle \delta \hat{x}_\mu^2 \rangle + \langle \hat{x}_\mu \rangle^2 \langle \delta \hat{x}_\nu^2 \rangle + \langle \hat{x}_\mu \rangle^2 \langle \hat{x}_\nu \rangle^2 + 4\langle \hat{x}_\mu \rangle \langle \hat{x}_\nu \rangle \langle \delta \hat{x}_\mu \delta \hat{x}_\nu \rangle + \langle \delta \hat{p}_\mu^2 \rangle \langle \delta \hat{p}_\nu^2 \rangle \\ &\quad + 2\langle \delta \hat{p}_\mu \delta \hat{p}_\nu \rangle^2 + \langle \hat{p}_\nu \rangle^2 \langle \delta \hat{p}_\mu^2 \rangle + \langle \hat{p}_\mu \rangle^2 \langle \delta \hat{p}_\nu^2 \rangle + \langle \hat{p}_\mu \rangle^2 \langle \hat{p}_\nu \rangle^2 + 4\langle \hat{p}_\mu \rangle \langle \hat{p}_\nu \rangle \langle \delta \hat{p}_\mu \delta \hat{p}_\nu \rangle + \langle \delta \hat{x}_\mu^2 \rangle \langle \delta \hat{p}_\nu^2 \rangle + 2\langle \delta \hat{x}_\mu \delta \hat{p}_\nu \rangle^2 \\ &\quad + \langle \hat{p}_\nu \rangle^2 \langle \delta \hat{x}_\mu^2 \rangle + \langle \hat{x}_\mu \rangle^2 \langle \delta \hat{p}_\nu^2 \rangle + \langle \hat{x}_\mu \rangle^2 \langle \hat{p}_\nu \rangle^2 + 4\langle \hat{x}_\mu \rangle \langle \hat{p}_\nu \rangle \langle \delta \hat{x}_\mu \delta \hat{p}_\nu \rangle + \langle \delta \hat{p}_\mu^2 \rangle \langle \delta \hat{x}_\nu^2 \rangle + 2\langle \delta \hat{p}_\mu \delta \hat{x}_\nu \rangle^2 + \langle \hat{x}_\nu \rangle^2 \langle \delta \hat{p}_\mu^2 \rangle \\ &\quad + \langle \hat{p}_\mu \rangle^2 \langle \delta \hat{x}_\nu^2 \rangle + \langle \hat{p}_\mu \rangle^2 \langle \hat{x}_\nu \rangle^2 + 4\langle \hat{p}_\mu \rangle \langle \hat{x}_\nu \rangle \langle \delta \hat{p}_\mu \delta \hat{x}_\nu \rangle - 2\langle \hat{x}_\mu^2 \rangle - 2\langle \hat{p}_\mu^2 \rangle. \end{aligned} \quad (\text{E11})$$

The second term, $4\langle n_\mu \rangle \langle n_\nu \rangle$, is given by:

$$\begin{aligned} 4\langle \hat{n}_\mu \rangle \langle \hat{n}_\nu \rangle &= 1 + \langle \delta \hat{x}_\mu^2 \rangle \langle \delta \hat{x}_\nu^2 \rangle + \langle \delta \hat{x}_\mu^2 \rangle \langle \hat{x}_\nu \rangle^2 + \langle \hat{x}_\mu \rangle^2 \langle \delta \hat{x}_\nu^2 \rangle + \langle \hat{x}_\mu \rangle^2 \langle \hat{x}_\nu \rangle^2 + \langle \delta \hat{p}_\mu^2 \rangle \langle \delta \hat{p}_\nu^2 \rangle + \langle \delta \hat{p}_\mu^2 \rangle \langle \hat{p}_\nu \rangle^2 + \langle \hat{p}_\mu \rangle^2 \langle \delta \hat{p}_\nu^2 \rangle \\ &\quad + \langle \hat{p}_\mu \rangle^2 \langle \hat{p}_\nu \rangle^2 + \langle \delta \hat{x}_\mu^2 \rangle \langle \delta \hat{p}_\nu^2 \rangle + \langle \delta \hat{x}_\mu^2 \rangle \langle \hat{p}_\nu \rangle^2 + \langle \hat{x}_\mu \rangle^2 \langle \delta \hat{p}_\nu^2 \rangle + \langle \hat{x}_\mu \rangle^2 \langle \hat{p}_\nu \rangle^2 + \langle \delta \hat{p}_\mu^2 \rangle \langle \delta \hat{x}_\nu^2 \rangle + \langle \delta \hat{p}_\mu^2 \rangle \langle \hat{x}_\nu \rangle^2 \\ &\quad + \langle \hat{p}_\mu \rangle^2 \langle \delta \hat{x}_\nu^2 \rangle + \langle \hat{p}_\mu \rangle^2 \langle \hat{x}_\nu \rangle^2 - 2\langle \delta \hat{x}_\mu^2 \rangle - 2\langle \hat{x}_\mu \rangle^2 - 2\langle \delta \hat{p}_\mu^2 \rangle - 2\langle \hat{p}_\mu \rangle^2. \end{aligned} \quad (\text{E12})$$

Finally, by combining both terms, the covariance of the number operators can be expressed as:

$$\begin{aligned} 4\text{cov}(\hat{n}_\mu, \hat{n}_\nu) &= 2[\langle \delta \hat{x}_\mu \delta \hat{x}_\nu \rangle^2 + \langle \delta \hat{p}_\mu \delta \hat{x}_\nu \rangle^2 + \langle \delta \hat{x}_\mu \delta \hat{p}_\nu \rangle^2 + \langle \delta \hat{p}_\mu \delta \hat{p}_\nu \rangle^2] \\ &\quad + 4[\langle \hat{x}_\mu \rangle \langle \hat{x}_\nu \rangle \langle \delta \hat{x}_\mu \delta \hat{x}_\nu \rangle + \langle \hat{p}_\mu \rangle \langle \hat{p}_\nu \rangle \langle \delta \hat{p}_\mu \delta \hat{p}_\nu \rangle + \langle \hat{x}_\mu \rangle \langle \hat{p}_\nu \rangle \langle \delta \hat{x}_\mu \delta \hat{p}_\nu \rangle + \langle \hat{p}_\mu \rangle \langle \hat{x}_\nu \rangle \langle \delta \hat{p}_\mu \delta \hat{x}_\nu \rangle] - \delta_{\mu\nu}, \end{aligned} \quad (\text{E13})$$

where the Kronecker delta $\delta_{\mu\nu}$ accounts for the noncommutativity of the quadrature operators. Therefore, the quantum Fisher information can be simply written in terms of the covariance matrix and first moments as:

$$\begin{aligned} \mathcal{Q}_{\mu\nu} &= 2(\sigma_{\hat{x}_\mu \hat{x}_\nu}^2 + \sigma_{\hat{p}_\mu \hat{p}_\nu}^2 + \sigma_{\hat{x}_\mu \hat{p}_\nu}^2 + \sigma_{\hat{p}_\mu \hat{x}_\nu}^2) + 4(\sigma_{\hat{x}_\mu \hat{x}_\nu} \bar{r}_{\hat{x}_\mu} \bar{r}_{\hat{x}_\nu} + \sigma_{\hat{p}_\mu \hat{p}_\nu} \bar{r}_{\hat{p}_\mu} \bar{r}_{\hat{p}_\nu} + \sigma_{\hat{x}_\mu \hat{p}_\nu} \bar{r}_{\hat{x}_\mu} \bar{r}_{\hat{p}_\nu} + \sigma_{\hat{p}_\mu \hat{x}_\nu} \bar{r}_{\hat{p}_\mu} \bar{r}_{\hat{x}_\nu}) - \delta_{\mu\nu} \\ &= 2 \sum_{z,w \in \{x,p\}} (\sigma_{\hat{z}_\mu \hat{w}_\nu}^2 + 2 \sigma_{\hat{z}_\mu \hat{w}_\nu} \bar{r}_{\hat{z}_\mu} \bar{r}_{\hat{w}_\nu}) - \delta_{\mu\nu}, \end{aligned} \quad (\text{E14})$$

where $\sigma_{\hat{z}_\alpha \hat{w}_\beta} := \langle (\hat{z}_\alpha - \bar{r}_{\hat{z}_\alpha})(\hat{w}_\beta - \bar{r}_{\hat{w}_\beta}) \rangle$ denotes the centered second moment and $\bar{r}_{\hat{z}_\alpha} = \langle \hat{z}_\alpha \rangle$. This concludes the proof of Lemma 2.

To prove Theorem 3, we begin by recalling the definition of the privacy measure: $P(\mathbf{v}_{\text{avg}}, \mathcal{Q}) = \mathbf{v}_{\text{avg}}^\top \mathcal{Q} \mathbf{v}_{\text{avg}} / \text{tr}(\mathcal{Q})$, where $\mathbf{v}_{\text{avg}} = (1, \dots, 1)^\top / \sqrt{M}$. Given the quantum Fisher information matrix $\mathcal{Q}$ derived in Lemma 2, the numerator of P can be written as

$$\mathbf{v}_{\text{avg}}^\top \mathcal{Q} \mathbf{v}_{\text{avg}} = \frac{1}{M} \sum_{\mu,\nu} \mathcal{Q}_{\mu\nu} = \frac{2}{M} \sum_{\mu,\nu} \sum_{z,w \in \{x,p\}} (\sigma_{\hat{z}_\mu \hat{w}_\nu}^2 + 2 \sigma_{\hat{z}_\mu \hat{w}_\nu} \bar{r}_{\hat{z}_\mu} \bar{r}_{\hat{w}_\nu}) - 1. \quad (\text{E15})$$

Similarly, the trace is given by $\text{tr}(\mathcal{Q}) = \sum_\mu \mathcal{Q}_{\mu\mu} = 2 \sum_\mu \sum_{z,w \in \{x,p\}} (\sigma_{\hat{z}_\mu \hat{w}_\mu}^2 + 2 \sigma_{\hat{z}_\mu \hat{w}_\mu} \bar{r}_{\hat{z}_\mu} \bar{r}_{\hat{w}_\mu}) - M$. Combining the numerator and the trace, we obtain the following closed-form expression for the privacy:

$$P(\mathbf{Q}, \mathbf{v}) = \frac{2 \sum_{\mu, \nu} \sum_{z, w \in \{x, p\}} (\sigma_{\hat{z}_\mu \hat{w}_\nu}^2 + 2 \sigma_{\hat{z}_\mu \hat{w}_\nu} \bar{r}_{\hat{z}_\mu} \bar{r}_{\hat{w}_\nu}) - M}{M[2 \sum_{\mu} \sum_{z, w \in \{x, p\}} (\sigma_{\hat{z}_\mu \hat{w}_\mu}^2 + 2 \sigma_{\hat{z}_\mu \hat{w}_\mu} \bar{r}_{\hat{z}_\mu} \bar{r}_{\hat{w}_\mu}) - M]}. \quad (\text{E16})$$

which proves Theorem 3.

APPENDIX F: NO COMPLETE AVERAGE-PHASE PRIVACY FOR GAUSSIAN PROBES

In this appendix we prove Theorem 4. For convenience, we first restate the theorem in a form adapted to the proof:

Theorem 4 restated. No rank-one average-phase QFI for Gaussian probes. Let $\hat{\rho}$ be an M -mode Gaussian state with $M \geq 3$, finite first moments $\bar{\mathbf{r}} \in \mathbb{R}^{2M}$ and covariance matrix $\sigma \in \mathbb{R}^{2M \times 2M}$. Consider the local phase-encoding family $\hat{\rho}(\theta) = \hat{U}(\theta) \hat{\rho} \hat{U}(\theta)^\dagger$ where $\hat{U}(\theta) = \prod_{\mu=1}^M e^{i\theta_\mu \hat{n}_\mu}$ with $\hat{n}_\mu = \hat{a}_\mu^\dagger \hat{a}_\mu$ and $\theta = (\theta_1, \dots, \theta_M)$. Let $\mathbf{Q}$ be the quantum Fisher information matrix of this family. If every direction orthogonal to the average-phase direction is unobservable, i.e.

$$\{\mathbf{u} \in \mathbb{R}^M : \mathbf{1}^\top \mathbf{u} = 0\} \subseteq \ker \mathbf{Q}, \quad \text{with } \mathbf{1} = (1, \dots, 1)^\top, \quad (\text{F1})$$

then $\mathbf{Q} = \mathbf{0}$. Consequently, no finite-energy Gaussian probe can satisfy $\text{rank } \mathbf{Q} = 1$ and $\text{range}(\mathbf{Q}) = \text{span}\{\mathbf{1}\}$. Equivalently, for $M \geq 3$ there is no Gaussian probe whose only nonzero local-phase sensitivity is the average phase $\mathbf{v}_{\text{avg}}^\top \theta$, with $\mathbf{v}_{\text{avg}} = \frac{1}{\sqrt{M}}$.

Proof. First note that no generality is lost by evaluating the QFI at $\theta = \mathbf{0}$. Since the local number operators commute, $\hat{U}(\theta_0 + \delta) = \hat{U}(\theta_0) \hat{U}(\delta)$, and hence $\hat{\rho}(\theta_0 + \delta) = \hat{U}(\theta_0) \hat{\rho}(\delta) \hat{U}(\theta_0)^\dagger$. The QFI is invariant under parameter-independent unitary conjugation, so $\mathbf{Q}(\theta_0) = \mathbf{Q}(\mathbf{0})$. We may therefore work at $\theta = \mathbf{0}$. Next, assume that the subspace $\mathcal{H}_0 := \{\mathbf{u} \in \mathbb{R}^M : \mathbf{1}^\top \mathbf{u} = 0\}$ is contained in $\ker \mathbf{Q}$. This subspace consists of all directions orthogonal to the average-phase direction. We now prove the result in three steps.

1. Step 1: vanishing QFI in all relative directions gives a relative-phase symmetry. For any $\mathbf{u} \in \mathbb{R}^M$, define

$$\hat{G}_u := \sum_{\mu=1}^M u_\mu \hat{n}_\mu. \quad (\text{F2})$$

Equivalently, consider the one-parameter curve through parameter space $\hat{\rho}_u(t) := \hat{\rho}(t\mathbf{u})$. This is not a restriction on the unknown parameters, but simply the directional submodel used to test sensitivity along $\mathbf{u}$. Since the number operators commute, $\hat{\rho}_u(t) = e^{it\hat{G}_u} \hat{\rho} e^{-it\hat{G}_u}$. The QFI of this one-parameter submodel is the obtained from the multiparameter

QFI, $F_Q[\hat{\rho}_u] = \mathbf{u}^\top \mathbf{Q} \mathbf{u}$. Thus, for every $\mathbf{u} \in \mathcal{H}_0 \subseteq \ker \mathbf{Q}$, the QFI in the direction $\mathbf{u}$ vanishes. By Lemma 8, in the regular Gaussian phase-estimation setting considered here this is equivalent to $\partial_u \hat{\rho}(\mathbf{0}) = 0$. For the present unitary encoding, $\partial_u \hat{\rho}(\mathbf{0}) = i[\hat{G}_u, \hat{\rho}]$. Hence $[\hat{G}_u, \hat{\rho}] = 0$ for all $\mathbf{u} \in \mathcal{H}_0$. Since this holds for every zero-sum vector, and since the number operators commute, it exponentiates to

$$\hat{U}(\phi) \hat{\rho} \hat{U}(\phi)^\dagger = \hat{\rho} \quad \text{for all } \phi \in \mathbb{R}^M \quad \text{with} \quad \mathbf{1}^\top \phi = 0. \quad (\text{F3})$$

2. Step 2: relative-phase invariance constrains the Gaussian moments. Let $\hat{\mathbf{r}} = (\hat{x}_1, \hat{p}_1, \dots, \hat{x}_M, \hat{p}_M)^\top$ be the quadrature vector. A local phase shift acts in phase space through the block-diagonal symplectic rotation $\hat{U}(\phi)^\dagger \hat{\mathbf{r}} \hat{U}(\phi) = \mathbf{S}(\phi) \hat{\mathbf{r}} \mathbf{S}(\phi) = \bigoplus_{\mu=1}^M R(\phi_\mu)$, where

$$R(t) = \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix}. \quad (\text{F4})$$

Therefore the Gaussian moments transform as $\bar{\mathbf{r}} \mapsto \mathbf{S}(\phi) \bar{\mathbf{r}}$ and $\sigma \mapsto \mathbf{S}(\phi) \sigma \mathbf{S}(\phi)^\top$. Using the invariance in Eq. (F3), we obtain

$$\bar{\mathbf{r}} = \mathbf{S}(\phi) \bar{\mathbf{r}} \quad \text{and} \quad \sigma = \mathbf{S}(\phi) \sigma \mathbf{S}(\phi)^\top \quad (\text{F5})$$

for every zero-sum phase vector ϕ . We write the first moments in mode blocks as $\bar{\mathbf{r}} = (\bar{\mathbf{r}}_1, \dots, \bar{\mathbf{r}}_M)$ with $\bar{\mathbf{r}}_\mu \in \mathbb{R}^2$ and decompose the covariance matrix into 2×2 blocks,

$$\sigma = \begin{pmatrix} \sigma_{11} & \cdots & \sigma_{1M} \\ \vdots & \ddots & \vdots \\ \sigma_{M1} & \cdots & \sigma_{MM} \end{pmatrix}, \quad \sigma_{\mu\nu} \in \mathbb{R}^{2 \times 2}. \quad (\text{F6})$$

First, we show that relative-phase invariance forces all first moments to vanish. For any mode μ and choose another mode $\ell \neq \mu$ and set $\phi_\mu = t$, $\phi_\ell = -t$ and $\phi_k = 0$ otherwise. This gives a zero-sum phase vector, so Eq. (F5) implies $\bar{\mathbf{r}}_\mu = R(t) \bar{\mathbf{r}}_\mu$ for all $t \in \mathbb{R}$. Differentiating at $t = 0$ gives $\mathbf{J} \bar{\mathbf{r}}_\mu = 0$. Because $\mathbf{J}$ is invertible, $\bar{\mathbf{r}}_\mu = \mathbf{0}$. As this holds for

every mode μ , we conclude that $\bar{\mathbf{r}} = \mathbf{0}$. Second, every diagonal covariance block is isotropic. Using the same zero-sum phase vector as above, Eq. (F5) implies $\sigma_{\mu\mu} = R(t)\sigma_{\mu\mu}R(t)^\top$ for all $t \in \mathbb{R}$. Differentiating at $t = 0$ gives $\mathbf{J}\sigma_{\mu\mu} - \sigma_{\mu\mu}\mathbf{J} = 0$. Writing the symmetric block as

$$\sigma_{\mu\mu} = \begin{pmatrix} a & b \\ b & c \end{pmatrix}, \quad (\text{F7})$$

one finds

$$\mathbf{J}\sigma_{\mu\mu} - \sigma_{\mu\mu}\mathbf{J} = \begin{pmatrix} -2b & a - c \\ a - c & 2b \end{pmatrix}. \quad (\text{F8})$$

Thus $b = 0$ and $a = c$, so $\sigma_{\mu\mu} = \nu_\mu \mathbb{1}_2$ for some $\nu_\mu \geq \frac{1}{2}$. Third, we show that relative-phase invariance forces all off-diagonal covariance blocks to vanish. For any distinct modes $\mu \neq \nu$, choose a third mode $\ell \neq \mu, \nu$ and set $\phi_\mu = t$, $\phi_\ell = -t$, and $\phi_\kappa = 0$ otherwise. This again gives a zero-sum phase vector, while mode ν is left unrotated. Equation (F5) then implies $\sigma_{\mu\nu} = R(t)\sigma_{\mu\nu}$ for all $t \in \mathbb{R}$. Differentiating at $t = 0$ gives $\mathbf{J}\sigma_{\mu\nu} = 0$. Because $\mathbf{J}$ is invertible $\sigma_{\mu\nu} = 0$. Since this holds for every pair of distinct modes $\mu \neq \nu$, all off-diagonal covariance blocks vanish. Combining the diagonal and off-diagonal constraints, the covariance matrix must have the form

$$\sigma = \bigoplus_{\mu=1}^M \nu_\mu \mathbb{1}_2 \quad \text{and} \quad \bar{\mathbf{r}} = \mathbf{0}. \quad (\text{F9})$$

3. Step 3: the state is then invariant under all local phase shifts. The form in Eq. (F9) is invariant under arbitrary local phase rotations, not only under zero-sum rotations. For every $\theta \in \mathbb{R}^M$, we have $\mathbf{S}(\theta)\bar{\mathbf{r}} = \bar{\mathbf{r}}$ and $\mathbf{S}(\theta)\sigma\mathbf{S}(\theta)^\top = \sigma$. Since a Gaussian state is completely determined by its first moments and covariance matrix, it follows that $\hat{U}(\theta)\hat{\rho}\hat{U}(\theta)^\dagger = \hat{\rho}$ for all $\theta \in \mathbb{R}^M$. Thus the encoded family is constant, so every local phase direction has zero QFI. Hence $\mathbf{Q} = \mathbf{0}$.

This proves that if all relative-phase directions lie in $\ker \mathbf{Q}$, then the average-phase direction also lies in $\ker \mathbf{Q}$. Hence $\ker \mathbf{Q} = \mathbb{R}^M$, and therefore $\mathbf{Q} = \mathbf{0}$. In particular, the only possible QFI with $\mathcal{H}_0 \subseteq \ker \mathbf{Q}$ is the zero matrix, so a nonzero rank-one QFI supported on $\text{span}\{\mathbf{1}\}$ cannot arise for an M -mode Gaussian probe with $M \geq 3$. ■

[1] P. Komar, E. M. Kessler, M. Bishof, L. Jiang, A. S. Sørensen, J. Ye, and M. D. Lukin, *A quantum network of clocks*, *Nat. Phys.* **10**, 582 (2014).

[2] H. Dai, Q. Shen, C.-Z. Wang, S.-L. Li, W.-Y. Liu, W.-Q. Cai, S.-K. Liao, J.-G. Ren, J. Yin, Y.-A. Chen, Q. Zhang, F. Xu, C.-Z. Peng, and J.-W. Pan, *Towards satellite-based quantum-secure time transfer*, *Nat. Phys.* **16**, 848 (2020).

[3] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, *Demonstration of blind quantum computing*, *Science* **335**, 303 (2012).

[4] J. F. Fitzsimons, *Private quantum computation: An introduction to blind quantum computing and related protocols*, *npj Quantum Inf.* **3**, 23 (2017).

[5] V. Giovannetti, S. Lloyd, and L. Maccone, *Quantum metrology*, *Phys. Rev. Lett.* **96**, 010401 (2006).

[6] Q. Zhuang, Z. Zhang, and J. H. Shapiro, *Distributed quantum sensing using continuous-variable multipartite entanglement*, *Phys. Rev. A* **97**, 032329 (2018).

[7] V. Giovannetti, S. Lloyd, and L. Maccone, *Quantum cryptographic ranging*, *J. Opt. B* **4**, S413 (2002).

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

[9] D. Gottesman, T. Jennewein, and S. Croke, *Longer-baseline telescopes using quantum repeaters*, *Phys. Rev. Lett.* **109**, 070503 (2012).

[10] T. Baumgratz and A. Datta, *Quantum enhanced estimation of a multidimensional field*, *Phys. Rev. Lett.* **116**, 030801 (2016).

[11] L.-Z. Liu, Y.-Z. Zhang, Z.-D. Li, R. Zhang, X.-F. Yin, Y.-Y. Fei, L. Li, N.-L. Liu, F. Xu, Y.-A. Chen, and J.-W. Pan, *Distributed quantum phase estimation with entangled photons*, *Nat. Photonics* **15**, 137 (2020).

[12] T. J. Proctor, P. A. Knott, and J. A. Dunningham, *Networked quantum sensing*, *arXiv:1702.04271*.

[13] T. J. Proctor, P. A. Knott, and J. A. Dunningham, *Multi-parameter estimation in networked quantum sensors*, *Phys. Rev. Lett.* **120**, 080501 (2018).

[14] W. Ge, K. Jacobs, Z. Eldredge, A. V. Gorshkov, and M. Foss-Feig, *Distributed quantum metrology with linear networks and separable inputs*, *Phys. Rev. Lett.* **121**, 043604 (2018).

[15] J. Rubio, P. A. Knott, T. J. Proctor, and J. A. Dunningham, *Quantum sensing networks for the estimation of linear functions*, *J. Phys. A* **53**, 344001 (2020).

[16] P. Sekatski, S. Wölk, and W. Dür, *Optimal distributed sensing in noisy environments*, *Phys. Rev. Res.* **2**, 023052 (2020).

[17] S. Wölk, P. Sekatski, and W. Dür, *Noisy distributed sensing in the Bayesian regime*, *Quantum Sci. Technol.* **5**, 045003 (2020).

[18] Z. Zhang and Q. Zhuang, *Distributed quantum sensing*, *Quantum Sci. Technol.* **6**, 043001 (2021).

[19] A. Hamann, P. Sekatski, and W. Dür, *Optimal distributed multi-parameter estimation in noisy environments*, *Quantum Sci. Technol.* **9**, 035005 (2024).

[20] N. Shettell, M. Hassani, and D. Markham, *Private network parameter estimation with quantum sensors*, *arXiv:2207.14450*.

[21] M. Hassani, S. Scheiner, M. G. A. Paris, and D. Markham, *Privacy in networks of quantum sensors*, *Phys. Rev. Lett.* **134**, 030802 (2025).

[22] X. Guo, C. R. Breum, J. Borregaard, S. Izumi, M. V. Larsen, T. Gehring, M. Christandl, J. S. Neergaard-Nielsen, and U. L. Andersen, *Distributed quantum sensing in a continuous-variable entangled network*, *Nat. Phys.* **16**, 281 (2020).

- [23] E. T. Khabiboulline, J. Borregaard, K. De Greve, and M. D. Lukin, *Optical interferometry with quantum networks*, *Phys. Rev. Lett.* **123**, 070504 (2019).
- [24] E. T. Khabiboulline, J. Borregaard, K. De Greve, and M. D. Lukin, *Quantum-assisted telescope arrays*, *Phys. Rev. A* **100**, 022316 (2019).
- [25] A. Unnikrishnan and D. Markham, *Verification of graph states in an untrusted network*, *Phys. Rev. A* **105**, 052420 (2022).
- [26] S. W. Moore and J. A. Dunningham, *Secure quantum-enhanced measurements on a network of sensors*, *Phys. Rev. A* **111**, 012616 (2025).
- [27] J. Ho, J. W. Webb, R. M. J. Brooks, F. Grasselli, E. Gauger, and A. Fedrizzi, *Quantum-private distributed sensing*, *J. Phys. Photonics* **8**, 025006 (2026).
- [28] L. Bugalho, M. Hassani, Y. Omar, and D. Markham, *Private and robust states for distributed quantum sensing*, *Quantum* **9**, 1596 (2025).
- [29] Y. Ueda, M. Ishihara, W. Roga, and M. Takeoka, *Quantum network sensing with efficient multi-partite entanglement distribution via lossy channels*, [arXiv:2505.10148](https://arxiv.org/abs/2505.10148).
- [30] G. Adesso and F. Illuminati, *Entanglement in continuous-variable systems: Recent advances and current perspectives*, *J. Phys. A* **40**, 7821 (2007).
- [31] H. Krauter, D. Salart, C. A. Muschik, J. M. Petersen, H. Shen, T. Fernholz, and E. S. Polzik, *Deterministic quantum teleportation between distant atomic objects*, *Nat. Phys.* **9**, 400 (2013).
- [32] U. Alushi and R. Di Candia, *Privacy in distributed quantum sensing with Gaussian quantum networks*, *npj Quantum Inf.* (2026).
- [33] M. G. A. Paris, *Quantum estimation for quantum technology*, *Int. J. Quantum Inf.* **07**, 125 (2009).
- [34] D. Safránek, *Simple expression for the quantum Fisher information matrix*, *Phys. Rev. A* **97**, 042322 (2018).
- [35] J. Liu, H. Yuan, X.-M. Lu, and X. Wang, *Quantum Fisher information matrix and multiparameter estimation*, *J. Phys. A* **53**, 023001 (2019).
- [36] L. J. Fiderer, T. Tufarelli, S. Piano, and G. Adesso, *General expressions for the quantum Fisher information matrix with applications to discrete quantum imaging*, *PRX Quantum* **2**, 020308 (2021).
- [37] S. Ragy, M. Jarzyna, and R. Demkowicz-Dobrzański, *Compatibility in multiparameter quantum metrology*, *Phys. Rev. A* **94**, 052108 (2016).
- [38] M. Szczykulska, T. Baumgratz, and A. Datta, *Multiparameter quantum metrology*, *Adv. Phys.* **1**, 621 (2016).
- [39] L. Seveso, F. Albarelli, M. G. Genoni, and M. G. A. Paris, *On the discontinuity of the quantum Fisher information for quantum statistical models with parameter dependent rank*, *J. Phys. A* **53**, 02LT01 (2020).
- [40] T. Gefen, A. Rotem, and A. Retzker, *Overcoming resolution limits with quantum sensing*, *Nat. Commun.* **10**, 4992 (2019).
- [41] J. W. Gardner, T. Gefen, S. A. Haine, J. J. Hope, J. Preskill, Y. Chen, and L. McCuller, *Stochastic waveform estimation at the fundamental quantum limit*, *PRX Quantum* **6**, 030311 (2025).
- [42] E. Descamps and D. Markham, *Noisy certification of continuous-variable graph states*, *Phys. Rev. A* **111**, 022413 (2025).
- [43] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, *Gaussian quantum information*, *Rev. Mod. Phys.* **84**, 621 (2012).
- [44] J. B. Brask, *Gaussian states and operations—A quick reference*, [arXiv:2102.05748](https://arxiv.org/abs/2102.05748).
- [45] A. Serafini, *Quantum Continuous Variables: A Primer of Theoretical Methods* (CRC press, Boca Raton, FL, 2023).
- [46] A. Monras, *Phase space formalism for quantum estimation of Gaussian states*, [arXiv:1303.3682](https://arxiv.org/abs/1303.3682).
- [47] A. de Oliveira Junior, *Privacy in continuous-variable distributed quantum sensing*, GitHub (2026).
- [48] L.-A. Wu, H. J. Kimble, J. L. Hall, and H. Wu, *Generation of squeezed states by parametric down conversion*, *Phys. Rev. Lett.* **57**, 2520 (1986).
- [49] R. E. Slusher, L. W. Hollberg, B. Yurke, J. C. Mertz, and J. F. Valley, *Observation of squeezed states generated by four-wave mixing in an optical cavity*, *Phys. Rev. Lett.* **55**, 2409 (1985).
- [50] J. L. Pereira and D. Markham, *A no-go theorem for privacy in distributed sensing using Gaussian states*, [arXiv:2606.23796](https://arxiv.org/abs/2606.23796).
- [51] M. F. B. Cenni, L. Lami, A. Acín, and M. Mehboudi, *Thermometry of Gaussian quantum systems using Gaussian measurements*, *Quantum* **6**, 743 (2022).
- [52] I. Bengtsson and K. Życzkowski, *Geometry of Quantum States: An Introduction to Quantum Entanglement* (Cambridge University Press, Cambridge, England, 2006).
- [53] M. E. Peskin, *An Introduction to Quantum Field Theory* (CRC press, 2018).