Quantum metrology with delegated tasks

Nathan Shettell and Damian Markham
LIP6, Centre National de la Recherche Scientifique, Sorbonne Université, 4 Place Jussieu, 75005 Paris, France

(Received 27 July 2022; accepted 7 November 2022; published 23 November 2022)

A quantum metrology scheme can be decomposed into three quantum tasks: state preparation, parameter encoding, and measurements. Consequently, it is imperative to have access to the technologies which can execute the aforementioned tasks to fully implement a quantum metrology scheme. In the absence of one or more of these technologies, one can proceed by delegating the tasks to a third party. However, doing so has security ramifications: the third party can bias the result or leak information. In this paper, we outline different scenarios where one or more tasks are delegated to an untrusted (and possibly malicious) third party. In each scenario, we outline cryptographic protocols which can be used to circumvent malicious activity. Further, we link the effectiveness of the quantum metrology scheme to the soundness of the cryptographic protocols.

DOI: 10.1103/PhysRevA.106.052427

I. MOTIVATION

Quantum metrology has witnessed a surge in interest over the past few years [1,2]. In brief, an unknown parameter is encoded into a quantum state through some interaction; consequently, the measurement statistics of an appropriately chosen positive operator-valued measure (POVM) will be dependent on said unknown parameter. With sufficient measurement data, an estimate of the unknown parameter can be constructed [3–5]. Quantum correlations make it possible to devise estimation strategies which attain a high level of precision, unobtainable through a classical means [6–10].

Fully implementing a quantum metrology scheme is technologically demanding. Quantum states must be initialized and measured with high fidelity. The quantum internet is a proposed networklike solution which can address the problem, amongst others, where parties which lack the necessary hardware can delegate the desired task to another party in the network [11]. Of course, when delegating tasks, it comes with security risks; we must deal with the fact that a malicious third party could bias the estimation results or extract information for their own benefit. It is therefore imperative to take proper cryptographic precautions when delegating a portion of a metrology scheme to an untrusted third party.

In the past few years, quantum cryptography has been introduced to quantum metrology to address possible security risks, such as unsecured quantum channels [12–15] and masking information from honest-but-curious eavesdroppers [16–18]. In this paper, we expand the repertoire of studied scenarios by considering the delegation of a portion of the quantum metrology process to an untrusted third party. We partition a quantum metrology problem into three tasks—state preparation, parameter encoding, and measurements—and explore the repercussions when a specific task, or a combination, is delegated. The different scenarios are summarized in Fig. 1. Note that there is an additional task of processing the measurement results and creating the estimate, however we ignore this since it is inherently a classical computation. We propose cryptographic protocols to circumvent malicious activity and achieve a sense of security for the scenarios of delegated state preparation and/or delegated measurements.

This paper builds upon [12], where we introduced different quantities to measure the effectiveness of the cryptographic protocol as well as the precision of the estimate related to the quantum metrology task, namely, integrity and soundness. Integrity is a measure of retaining functionality in the presence of a malicious adversary, whereas soundness provides a notion of security as it measures the ability of successfully detecting malicious activity, and thus it measures how much one can trust the resource in question. Two of the scenarios explored in this paper are concerned with delegated quantum measurements, i.e., (potentially malicious) classical information, as such we have extended the mathematical definitions of integrity and soundness to allow for this possibility. Furthermore, the cryptographic protocols showcased in [12] use tools from quantum message authentication schemes [19,20]; in this paper we show that a similar protocol can be used for the delegation of certain tasks; additionally we show that quantum state verification [21–24] can also be adapted within cryptographic quantum metrology. Finally, in this paper, we demonstrate the impossibility of delegating the task of parameter encoding in an information theoretic manner.

II. PRELIMINARIES

A. Soundness of a cryptographic protocol

The field of quantum cryptography is extremely broad in functionality and perspectives [25,26]. Ergo, a suitable figure of merit for a cryptographic protocol must be relevant for the scope of the protocol and provide a notion of comparability between similar protocols. In the domain of quantum verification and authentication [25,27,28]—for

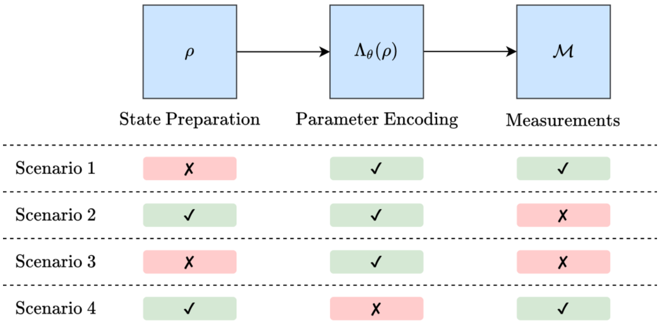

FIG. 1. The different delegated quantum metrology scenarios we address in this paper. A quantum metrology problem can be decomposed into three (quantum) tasks: state preparation, parameter encoding, and measurements. As a whole, this is technologically demanding and it may be necessary to delegate one or more of these tasks to a third party. In this paper we explore four different scenarios, each motivated through the necessity to delegate a task to a third party due to the lack of specific hardware. A red rectangle with an x mark indicates that the task is delegated to a third party, as opposed to a green rectangle with a check mark which indicates that the task is not delegated. In scenario 1, state preparation is delegated and we use verification protocols [22,23] to achieve a sense of security. In scenario 2, the measurements are delegated and we devise an authentication based protocol to achieve a sense of security. In scenario 3, both state preparation and measurements are delegated, and we discuss the criteria for when both of the aforementioned protocols can be used in tandem to achieve a sense of security. Finally, in scenario 4, the parameter encoding is delegated, and we discuss the impossibility of constructing a computationally secure protocol.

example quantum states [22,23], quantum messages [19], or quantum computations [29]—a common figure of merit is soundness. The soundness of a protocol gives a notion of security as it quantifies the ability of successfully detecting alterations made by a malicious adversary and how much we can trust the resource in question. The formal mathematical definition of soundness varies depending on the formulation of the cryptographic protocol [19,22,23,29,30], and is sometimes referred to as verifiability [27]. For the sake of continuity, we use the same definition of soundness as we did in [12], which is a slightly modified version of the definition presented in [19], as they are suited to our problem, and similar statements can be made for other variants of the definition.

Verification protocols have two outputs. One is a binary accept or reject clause. The other will be a quantum state, which can be understood as either an output in its own right or an encoding of a classical measurement result [see Eq. (11)]. The protocols we define are equipped with ancillary qubits, which are designed to have a deterministic measurement outcome in an ideal scenario in which the untrusted party behaves as intended; if the expected measurement result is observed we assign the outcome of *accept* to the protocol. However, if an unexpected result is observed, one can conclude that the untrusted third party acted maliciously and we assign the outcome of *reject* to the protocol. To achieve information theoretic security, the untrusted party is assumed to be able to perform any allowable operation and is completely familiar with the protocol. In order to deal with a malicious adversary, the protocols are supported by a set of classical keys $\mathcal{K}$, where each key alters the protocol differently. A different key is chosen at random for each implementation of the protocol, and even though the adversary may have access to a set of possible keys, they do not have access to the specific choice of key for any given implementation.

The formal definition of soundness is a bound on the probability of *accept*, while the output quantum state $\rho_{\rm out}$ is simultaneously far from the ideal output ($\rho_{\rm id}$). In [19] the protocol is designed $\rho_{\rm id}$ being a pure state, and the distance is recorded as $\mathrm{Tr}(\rho_{\rm id}\rho_{\rm out})$. In order to generalize this concept to mixed states, our version of soundness used the fidelity $F(\rho_{\rm id},\rho_{\rm out}) = (\mathrm{Tr}\sqrt{\sqrt{\rho_{\rm id}}\rho_{\rm out}\sqrt{\rho_{\rm id}}})^2$. We say a protocol has soundness δ if

$$\frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}} p_{\rm acc}(k,\Gamma)\cdot[1-F(\rho_{\rm id},\rho_{\rm out}(k,\Gamma))]\leqslant\delta. \qquad (1)$$

Here, Γ represents any possible attack a malicious adversary may perform, and $k\in\mathcal{K}$ is the specific key chosen. The probability of the protocol outputting *accept*, $p_{\rm acc}(k,\Gamma)$, and the output $\rho_{\rm out}(k,\Gamma)$ is dependent on both of these quantities. Equation (1) must hold for all Γ.

In the instance that $p_{\rm acc}(k,\Gamma)\geqslant\alpha$, then Eq. (1) can be written to read

$$1-\mathbb{E}(F(\rho_{\rm id},\rho_{\rm out}))\leqslant\frac{\delta}{\alpha}, \qquad (2)$$

where $\mathbb{E}$ denotes the expected value and we have omitted the dependence of $\rho_{\rm out}$ on the key k and the attack Γ for clarity. The quantity α is sometimes referred to as the statistical significance [22,23]. More so, this formalization easily permits the construction of additional figures of merit which are intertwined with the soundness and statistical significance [22,23]. To connect the soundness of a cryptographic protocol to the utility of $\rho_{\rm out}$ for quantum metrology, we write Eq. (2) in terms of the trace distance $\mathcal{D}(\rho_{\rm id},\rho_{\rm out})=\frac{1}{2}\mathrm{Tr}|\rho_{\rm id}-\rho_{\rm out}|$ [12]. This is done using the arithmetic-quadratic mean inequality and the Fuchs–van de Graaf inequalities [31]:

$$\begin{aligned}\mathbb{E}[\mathcal{D}(\rho_{\rm id},\rho_{\rm out})] &\leqslant \sqrt{\mathbb{E}[\mathcal{D}(\rho_{\rm id},\rho_{\rm out})^2]}\\ &\leqslant \sqrt{1-\mathbb{E}[F(\rho_{\rm id},\rho_{\rm out})]}\\ &\leqslant \sqrt{\frac{\delta}{\alpha}}. \end{aligned} \qquad (3)$$

B. Privacy

Privacy is a straightforward concept which quantifies the amount of information a malicious eavesdropper can extract from a message (quantum or otherwise). The protocols outlined in this paper are all completely private, which is to say that an eavesdropper can extract no information about an encoded parameter. If an eavesdropper can access the quantum state ρ_E, then this is achieved if

$$\mathbb{E}(\rho_E)=\mathbb{I}/d, \qquad (4)$$

where d is the dimension of ρ_E. Thus, a protocol is completely private when the expected quantum state accessible to an eavesdropper is indistinguishable from the maximally mixed state.

C. Quantum metrology

In quantum metrology, an unknown parameter θ is encoded into an initialized quantum state ρ through some completely positive trace-preserving (CPTP) map Λ_θ; the encoded quantum state $\rho_\theta = \Lambda_\theta(\rho)$ is then measured with respect to some POVM $\mathcal{M}$. If $\mathcal{M}$ is appropriately chosen, the measurement result will be dependent on θ, and if the prepare, encode, and measure protocol is repeated sufficiently many times, $\nu \gg 1$, the measurement statistics can be used to construct an estimate $\hat{\theta}$. Formally, $\hat{\theta}$ is called an estimator and should be thought of as a function of the measurement results the output of which is an estimate of θ [32].

An estimator is said to be unbiased if $\mathbb{E}(\hat{\theta}) = \theta$. In classical estimation theory, the ultimate precision of an unbiased estimator is limited by the Cramér-Rao bound [33]. In the realm of quantum estimation theory [34,35], the ultimate precision is further enhanced by optimizing over all possible POVMs [36]:

$$\Delta^2\hat{\theta} = \mathbb{E}((\hat{\theta} - \theta)^2) \geqslant \frac{1}{\nu \mathcal{Q}}, \tag{5}$$

where $\mathcal{Q}$ is the quantum Fisher information (QFI). The QFI is a measure of how much information of θ is contained within ρ_θ; it is defined as

$$\mathcal{Q} = \mathrm{Tr}(\rho_\theta L^2), \tag{6}$$

where L is the symmetric logarithmic derivative which satisfies

$$\partial_\theta \rho_\theta = \frac{1}{2}(L\rho_\theta + \rho_\theta L). \tag{7}$$

It is always possible to saturate the quantum Cramér-Rao bound, Eq. (5), by measuring in the eigenbasis of L [36]. However, this measurement is often complex and inherently dependent on θ. A more practical approach is to infer $\hat{\theta}$ from an estimate of the expectation value of an observable O. Suppose O has eigenbasis $\{|\psi_j\rangle\}$ with associated eigenvalues $\{o_j\}$. If the kth measurement results in $|\psi_j\rangle$, by setting $m_k = o_j$ the maximum likelihood estimate [5] is

$$\langle \hat{O} \rangle = \frac{1}{\nu}\sum_{k=1}^{\nu} m_k. \tag{8}$$

The symbol $\langle \hat{O} \rangle$ represents an estimate of the quantity $\langle O \rangle = \mathrm{Tr}(O\rho_\theta)$. To avoid confusion between $\langle \square \rangle$ and $\mathbb{E}(\square)$, we exclusively use $\mathbb{E}(\square)$ for (classical) statistical quantities. The estimate of $\langle \hat{O} \rangle$ can be inverted to obtain an estimate $\hat{\theta}$. By the central limit theorem, as ν increases, $\langle \hat{O} \rangle$ will fluctuate closer and closer to the true value $\langle O \rangle$. Thus, the first-order Taylor approximation

$$\hat{\theta} \approx \theta + \frac{1}{|\partial_\theta \langle O \rangle|}(\langle \hat{O} \rangle - \langle O \rangle) \tag{9}$$

is assumed to be a valid approximation, which is used to compute the error propagation formula

$$\Delta^2\hat{\theta} = \frac{\Delta^2\langle \hat{O} \rangle}{|\partial_\theta \langle O \rangle|^2} = \frac{\Delta^2 O}{\nu |\partial_\theta \langle O \rangle|^2}, \tag{10}$$

where $\Delta^2 O = \mathrm{Tr}(O^2\rho_\theta) - \mathrm{Tr}(O\rho_\theta)^2$.

Critically, quantum effects can lead to an advantage in precision compared to the best classical strategies [37,38]. For example by initializing an n qubit Greenberger-Horne-Zeilinger (GHZ) state, and encoding a phase θ identically on each individual qubit, then by choosing $O = X^{\otimes n}$, one calculates $\Delta^2\hat{\theta} = \frac{1}{\nu n^2}$ [5]. The quadratic scaling in n is otherwise known as the Heisenberg limit and is the ultimate bound in precision allowable with quantum strategies [4,37].

D. Cryptographic quantum metrology

In a cryptographic framework, many of the previously described notions from estimation theory are no longer applicable. If there is possibility that a malicious adversary tampers with any of the quantum processes (state preparation, encoding, or measurements) then there is no guarantee that the estimator will remain unbiased. Thus, there is no guarantee that the QFI is even attainable; as such the QFI is not a practical figure of merit in the realm of cryptographic quantum metrology. Instead, it is simpler to focus on a specific estimation strategy, such as the aforementioned method inferring an estimate by measuring an observable, and compare the estimate precision in the cryptographic framework to the estimate precision in the ideal framework (no malicious adversary). Because of the possibility of malicious tampering, the precision can be worse in the cryptographic setting. To fit the language of statistics, the cryptographic framework of quantum metrology injects uncertainty into the estimate. This additional uncertainty can be bounded by taking proper precautions and employing appropriate cryptographic protocols. For an estimate to be practical, the expected measurement statistics in the cryptographic framework must resemble the measurement statistics in the ideal framework. It will be shown that such a claim can be made by implementing appropriate cryptographic protocols. For simplicity, we restrict measurements to projection-valued measurements. We define the expected measurement statistics as a statistical ensemble $\mathcal{M}(\rho_\theta)$ (a mixed state with no coherence terms). In the ideal case, the encoded quantum state ρ_θ is measured in an orthonormal basis $\{\psi_j\}$ and the expected measurement statistics are

$$\mathcal{M}(\rho_\theta) = \sum_j |\psi_j\rangle\langle\psi_j|\rho_\theta|\psi_j\rangle\langle\psi_j|. \tag{11}$$

As the prepare, encode, and measure protocol is repeated ν times, the overall expected measurement statistics is $\mathcal{M}(\rho_\theta)^{\otimes \nu}$. In contrast, there is no guarantee that the expected measurement statistics are known. Further, they are not guaranteed to be dependent on θ. Without loss of generality, they can be expressed as $\mathcal{M}(\rho'^{(k)})$ to be the statistics of the kth round of the prepare, encode, and measure protocol. We demand that

$$\frac{1}{\nu}\sum_{k=1}^{\nu} \mathcal{D}(\mathcal{M}(\rho_\theta), \mathcal{M}(\rho'^{(k)})) \leqslant \varepsilon, \tag{12}$$

where $\mathcal{D}$ is the trace distance and ε is an adjustable parameter. In [12] we define a similar bound, but with respect to ρ_θ and $\rho'^{(k)}$; as this paper explores delegated measurement, this modification is necessary. In fact, this is a stronger bound than what is presented in [12] because the trace distance is contractive under CPTP maps.

For $\varepsilon \ll 1$, the most sensible strategy in the cryptographic framework is the same one as the ideal framework. That is to use the measurement results $m_1', \ldots, m_\nu'$, where $\mathbb{E}(m_k') = \mathrm{Tr}(O\rho'^{(k)}) = \mathrm{Tr}[O\mathcal{M}(\rho'^{(k)})]$, to construct an $\langle \hat{O} \rangle'$ and invert it to obtain $\hat{\theta}'$. We use the notation $\square'$ to indicate a quantity $\square$ in the cryptographic framework. Assuming that ε is small enough such that the Taylor approximation Eq. (9) is still valid in the cryptographic framework, then the precision is now the sum of the variance and a bias:

$$\begin{aligned}\Delta^2\hat{\theta}' &= \mathbb{E}\{[\hat{\theta}' - \mathbb{E}(\hat{\theta}') + \mathbb{E}(\hat{\theta}') - \theta]^2\}\\ &= \mathbb{E}\{[\hat{\theta}' - \mathbb{E}(\hat{\theta}')]^2\} + [\mathbb{E}(\hat{\theta}') - \theta]^2. \qquad (13)\end{aligned}$$

As a consequence of the stronger bound Eq. (12) than what is presented in [12], the same proofs presented in [12] hold in which we show that the bias is bounded by

$$|\mathbb{E}(\hat{\theta}') - \theta| \leqslant \frac{2o\varepsilon}{|\partial_\theta \langle O \rangle|}, \qquad (14)$$

and the integrity is bounded by

$$|\Delta^2\hat{\theta}' - \Delta^2\hat{\theta}| \leqslant \frac{4o^2(2\nu^{-1}\varepsilon + \varepsilon^2)}{|\partial_\theta \langle O \rangle|^2}, \qquad (15)$$

where o is the maximum magnitude of the eigenvalues of O. It follows that, in order for the metrology task to maintain a similar functionality in the cryptographic framework, the bias and variance must scale appropriately, namely,

$$\mathcal{O}(\Delta^2\theta') = \mathcal{O}(\Delta^2\theta), \qquad (16)$$

for which we must have that $\varepsilon^2 \leqslant \nu^{-1}$. Depending on the setting, one may relax this condition, for example, if one is primarily interested in security. In our case we will address the question of resources in the strongest case, which is to also match the scaling for accuracy.

Finally, we combine the soundness of a cryptographic protocol, Eq. (2), with the restriction on the measurement statistics Eq. (12). As was previously mentioned, even if the output of a cryptographic protocol ρ_{out} is a quantum state, the bound on the measurement statistics is still valid because of the concavity of the trace distance under CPTP maps. Hence, if a cryptographic protocol with soundness δ and statistical significance α is used in a cryptographic metrology scheme, for each prepare, encode, and measure round, then the bias, Eq. (14), and integrity, Eq. (15), are bounded with $\varepsilon = \sqrt{\frac{\delta}{\alpha}}$, where we have made the assumption that the ν output states $\rho_{\mathrm{out}}^{(1)}, \ldots, \rho_{\mathrm{out}}^{(\nu)}$ follow the law of large numbers:

$$\frac{1}{\nu}\sum_{k=1}^{\nu} \mathcal{D}\big(\rho_{\mathrm{id}}, \rho_{\mathrm{out}}^{(k)}\big) \approx \mathbb{E}[\mathcal{D}(\rho_{\mathrm{id}}, \rho_{\mathrm{out}})]. \qquad (17)$$

III. DELEGATED STATE PREPARATION

The first scenario we explore is when the task of quantum state preparation is delegated to an untrusted party. In the absence of a proper cryptographic protocol, the untrusted party could distribute any quantum state ρ', which could be preemptively biased to mask the true result of the parameter estimation. Fortunately, there exists a plethora of existing quantum state verification protocols [21–24,30,39,40], which ensure the quantum state prepared is the desired quantum state.

Verification protocols are used to (as the name suggests) verify quantum states. Typically, this is done by requesting additional copies of the desired quantum state and by measuring the additional copies in specific bases. The measurement results are used to decide if the protocol is accepted or rejected. It should be noted that most verification protocols are tailored for specific classes of quantum states, such as graph states [24,30] or Dicke states [40]. More general protocols tend to require significantly more resources to achieve the same level of soundness for arbitrary quantum states [21,39].

As an example, consider the graph state verification protocol outlined in [24]. The protocol extends to any stabilizer state, which has been shown to be a useful class of states for quantum metrology [41], specifically the GHZ state which is the canonical resource for phase estimation [4,5]. The protocol takes advantage of the deterministic measurement results when measuring in a stabilizer basis [42]. In summary, N copies of the desired quantum state are requested, and all but one (randomly selected) is measured with respect to a random stabilizer. The protocol achieves a soundness of $\delta = 1/N$. Therefore, if the verification protocol in [24] is incorporated into a cryptographic quantum metrology scheme, we must have that

$$\frac{1}{\alpha N} \leqslant \frac{1}{\nu} \Rightarrow N \geqslant \frac{\nu}{\alpha}, \qquad (18)$$

to maintain a similar level of precision. After ν repetitions of the prepare, encode, and measure part of the quantum metrology scheme, this translates to a total of $\mathcal{O}(\nu^2/\alpha)$ requested quantum states, or a quadratic increase in resources compared to the ideal framework.

IV. DELEGATED MEASUREMENTS

The next scenario we explore is when the measurements are delegated to an untrusted third party. A setting with an honest-but-curious adversary was explored in [16–18] where the authors utilized tools from blind quantum computing [43] to hide the measurement results from an eavesdropper. In our version, we do not utilize the traditional blind quantum computing protocol, as it is designed solely to guarantee privacy, i.e., hide the input and output of the computation (which is the measurement in this instance), and assumes that the computation is carried out honestly. We make no assumptions about the untrusted party; for all intents and purposes the untrusted party may return arbitrary measurement results and attempt to gain information about the encoded parameter. Therefore, without proper precautions, a malicious adversary could send tailored measurement results so that the constructed estimate is a specific value of their own interest. To combat this we take inspiration from verified blind quantum computing [29,44] and modify the protocols we developed for performing quantum metrology over an unsecured quantum channel [12] to accommodate the output being a set of measurement results.

We designate Alice as the trusted party who lacks the necessary quantum technologies to execute a quantum measurement. There could be several practical reasons for this. Depending on the physical systems used measurement devices

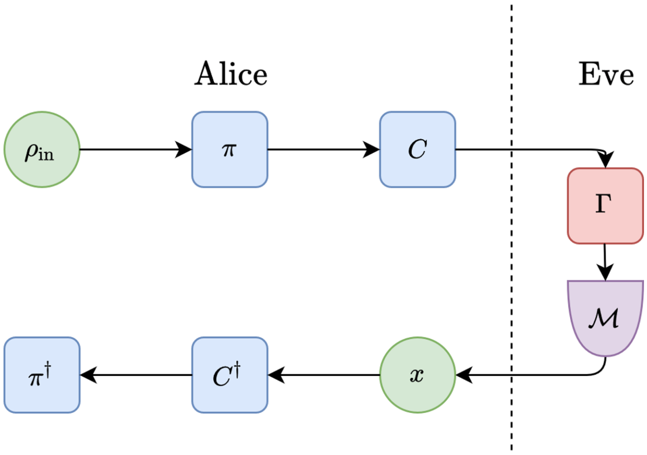

FIG. 2. Before sending a quantum state to Eve to be measured, Alice can attain a sense of security by employing our protocol. In summary, Alice prepares a quantum state, ρ_{in}, which is a combination of the qubits intended from quantum metrology as well as ancillary flag qubits. Alice then encrypts the quantum state by performing a permutation π and a Clifford operation C. The measurement result x returned by Eve is, without loss of generality, completely arbitrary. But for all intents and purposes we write that it stems from the measurement statistics as if Eve performed the requested measurement $\mathcal{M}$ after performing an arbitrary attack Γ. Alice will perform postprocessing on x to correctly interpret the result, i.e., decrypt the result by inverting the Clifford operation undoing the permutation. Alice accepts the result if the measurement result of the ancillary flag qubits corresponds to the expected result.

themselves can be bulky, expensive affairs, such as detectors requiring cryogenic cooling, and for example Alice may be constrained to small devices, for example using optical chips so that they are portable. Furthermore, ultimately we imagine such delegation to be used in different settings in conjunction with other constraints and tasks, and so for flexibility it is prudent to consider all cases.

Alice delegates the measurement task to Eve, who will return the measurement results to Alice. Alice can then use the measurement results to construct an estimate of the unknown parameter. In an ideal setting where Eve acts honestly, Alice sends many copies of an n qubit encoded quantum state ρ_θ to Eve, and requests that Eve performs a specific projective-valued measurement on each copy of of the quantum state. Eve returns the measurement results to Alice, which stems from the statistical ensemble $\mathcal{M}_{\text{id}}(\rho_\theta)$. In the (potentially) malicious setting, the measurement results stem from an arbitrary $\mathcal{M}_{\text{id}}(\rho')$. To ensure a sense of security and privacy, Alice uses a cryptographic protocol, which is described below and illustrated in Fig. 2.

The protocol described below is designed solely for the case when the ideal measurement $\mathcal{M}_{\text{id}}$ corresponds to measuring each qubit with respect to a Pauli basis. It can be adapted to other nonentangled measurements by appropriately rotating the encryption operations. Entangled measurements could also be considered, but would require encoding over more systems. We focus on simple measurement strategies as they are the simplest to implement and the encryption strategy requires only local Clifford operations. The Clifford group is a set of unitary operations which normalize the Pauli group up to a phase of ± 1. Thus, for any Clifford C and $P \in \{X, Y, Z\}$

$$CPC^\dagger \in \{\pm X, \pm Y, \pm Z\}. \tag{19}$$

The set of locally acting Clifford operations, $\mathcal{C}_1$, can be simulated efficiently on a classical computer [45] and implemented using only sequences of $\pi/4$ rotations.

The protocol is as follows.

(1) Alice prepares the $m = n + t$ qubit state $\rho_{\text{in}} = \rho_\theta \otimes |0\rangle\langle 0|^{\otimes t}$. Here, ρ_θ is the n qubit quantum state where the unknown parameter θ has already been encoded, and the additional t flag qubits, each initialized as $|0\rangle$, act as traps because of their deterministic measurement outcome.

(2) Alice encrypts ρ_{in} by first performing a permutation π and then applies a random Clifford $C \in \mathcal{C}_1^{\otimes m}$, $\rho_{\text{in}} \rightarrow \tilde{\rho} = C\pi\rho_{\text{in}}\pi^\dagger C^\dagger$. The permutation will insert the flag qubits at random positions so that Eve cannot distinguish between encoded qubits and flag qubits, and (as we will show) applying a random Clifford will guarantee privacy. Alice sends the permuted and encrypted quantum state to Eve.

(3) In the ideal case, Alice would request Eve to perform the measurement $\mathcal{M}_{\text{id}}$, which has Eve measuring the n qubits for quantum metrology in the eigenbasis of some Pauli operator and the flag qubits in the computational basis. We write that the set of projectors which correspond to $\mathcal{M}_{\text{id}}$ is $\{E\}$. In the potentially malicious case, Alice requests Eve to perform the measurement $\mathcal{M}$, which has corresponding projectors $\{C\pi E\pi^\dagger C^\dagger\}$. Doing so prevents Eve from distinguishing between a trap qubit and a qubit intended for metrology.

(4) Eve returns a measurement result x to Alice. Without loss of generality, this measurement result originates from the measurement statistics of $\mathcal{M}[\Gamma(\tilde{\rho})]$, where Γ is any CPTP map which represents an attack performed by Eve.

(5) Alice performs classical postprocessing on the measurement results to obtain the measurement result as if it had not been encrypted or permuted. When converted, the result will correspond to an outcome from the measurement statistics $\pi^\dagger C^\dagger \mathcal{M}[\Gamma(\tilde{\rho})]C\pi$.

(6) Alice accepts the measurement results if, after postprocessing, the measurement results of the t flag qubits coincided with the expected result of $|0\rangle\langle 0|^{\otimes t}$. Otherwise, Alice rejects the measurement results as Eve must acted maliciously.

The reason the protocol is designed for Pauli measurements (in the ideal case) is because a random local Clifford will map each qubit to be measured in an equal distribution of measuring in the eigenbasis of X, Y, or Z, as well as possibly flip the expected results. This encoding prevents Eve from distinguishing the flag qubits and the metrology qubits. As a result, the protocol is completely private, and Eve cannot learn any information from the measurement results. The expected quantum state Eve receives is equivalent to the maximally mixed state:

$$\mathbb{E}(\tilde{\rho}) = \frac{\mathbb{I}}{2^m}. \tag{20}$$

A proof is given in Appendix B.

For a general measurement, it is not necessarily true that a locally acting Clifford C will make the requested measurement indiscernible from the measurements on the flag qubits. The protocol can be generalized for more complex measurement strategies (e.g., measuring in a basis with inherent entanglement) by designing encryption operations in tandem with appropriately chosen flag qubits such that Eve cannot extract any information about the encoding from the requested measurement.

We show in Appendix B that our protocol achieves a soundness of $\delta = \frac{3n}{2t}$. Therefore, to maintain a similar level of precision in the cryptographic framework, we must have that

$$\frac{3n}{2\alpha t} \leqslant \frac{1}{\nu} \Rightarrow t \geqslant \frac{3n\nu}{2\alpha}. \tag{21}$$

After ν repetitions of the prepare, encode, and measure part of the quantum metrology scheme, this translates to an additional $\mathcal{O}(3n\nu^2/2\alpha)$ number of qubits, or a quadratic increase compared to the ideal framework.

V. DELEGATED STATE PREPARATION AND MEASUREMENTS

The third scenario we consider is when both the quantum state preparation and the measurements are delegated to untrusted parties. This scenario is motivated by quantum sensing networks, where a central node in the network distributes the quantum states for sensing throughout a quantum network, and encoded quantum states are returned to the central node for measurement [15,46]. If the central node is untrusted, it is necessary for the outer nodes to incorporate a cryptographic protocol.

We continue to use the same notation introduced in the last scenario, where Alice is the trusted party and Eve is the untrusted party. Although it is plausible that the party tasked with state preparation is different than the party tasked with measurement, this distinction is irrelevant in the grand scheme of the soundness proof. Further, assuming that they are the same party results in a stronger security analysis.

In this scenario, we again restrict the requested measurement to be in a Pauli basis. We impose two additional restrictions: the first is that the requested quantum state is a stabilizer state, since it can be efficiently verified using single-qubit measurements [24,30]; the second is that the encoding map is a local unitary operation, i.e., $\Lambda_\theta \rightarrow U_\theta^{\otimes n}$. In reality, these restrictions can be loosened.

(i) The requested measurement can be any single-qubit measurement scheme, and to compensate the encryption must be appropriately altered.

(ii) The requested quantum state can be any quantum state which can be verified using a single-qubit measurement strategy; however, without establishing the quantum state the protocol is quite vague, and it may not be possible to bound the soundness.

(iii) The nature of Λ_θ should have little to no impact on the soundness, however the third assumption is necessary to obtain a bound on the soundness. To execute the protocol, it is assumed that Alice can perform local Clifford operations.

The protocol is as follows.

(1) Alice requests that Eve prepare N copies of an n qubit stabilizer state ρ, hence $\rho^{\otimes N}$.

(2) Eve sends an Nn qubit state ρ' to Alice.

(3) Alice randomly chooses a positive integer $l \leqslant N$; this index represents the block of n qubits which Alice encodes the unknown parameter onto. As the encoding map is restricted to local unitaries, this is represented by $U^{(l)} = \mathbb{I}^{\otimes n(l-1)} \otimes U_\theta^{\otimes n} \otimes \mathbb{I}^{\otimes n(N-l)}$. After encoding the unknown parameter, the quantum state Alice possesses is $U^{(l)}\rho' U^{(l)\dagger}$.

(4) Alice randomly selects random Clifford operations $C_1, \ldots, C_N \in \mathcal{C}_1^{\otimes n}$. Alice encrypts the encoded quantum state using $C = \otimes_{j=1}^{N} C_j$.

(5) Alice randomly chooses $N-1$ stabilizers from the stabilizer group of ρ, $S_1, \ldots, S_{l-1}, S_{l+1}, \ldots, S_N$.

(6) Alice sends the encoded and encrypted quantum state to Eve for measurements. Alice requests each of the N blocks of n qubits to be measured with respect to a specific measurement $\mathcal{M}_j$. For $j = l$, $\mathcal{M}_l$ has corresponding projectors $\{C_l E C_l^\dagger\}$, where $\{E\}$ is the set of projectors of the ideal measurement. If $j \neq l$, $\mathcal{M}_j$ corresponds to measuring in the basis of $C_j S_j C_j^\dagger$ (note that if $C_j S_j C_j^\dagger$ has identity terms at certain indices then Alice requests those qubits to be measured with respect to a random Pauli basis; this will not effect the non-identity terms of the stabilizer measurement and prevent Eve from discerning between $j = l$ and $j \neq l$). For conciseness, the total measurement is labeled as $\mathcal{M} = \bigotimes_{j=1}^{N} \mathcal{M}_j$.

(7) Eve returns the measurement results $x_1, \ldots, x_N$. Without loss of generality these measurements originate from the measurement statistics of Eve performing an attack Γ on the quantum state they receive and then performing the requested measurement $\mathcal{M}$.

(8) Alice performs classical postprocessing to obtain the measurement results as if they had not been encrypted.

(9) Alice accepts the measurement results if (after postprocessing) each x_j with $j \neq l$ corresponds to a $+1$ eigenvalue of S_j. Otherwise, Alice rejects the measurement results as Eve must have acted maliciously in either the state preparation or the measurements (or both).

In addition to the three aforementioned assumptions made with respect to this scenario, we also assume that Eve cannot alter the state between step 3 and step 4 of the protocol. This is to prevent Eve from obtaining information about θ before Alice encrypts the quantum state. With the above assumption, the reason the protocol, illustrated in Fig. 3, achieves a sense of security is because in step 6, from Eve's perspective each $\mathcal{M}_j$ is indistinguishable from measuring each qubit with respect to the basis of a random Pauli. More so, even if Eve randomly guesses l correctly, the measurement results are still encrypted such that Eve cannot extract any information about θ. Consequently, the expected quantum state after the encryption is the maximally mixed state and thus the protocol is completely private:

$$\mathbb{E}(CU^{(l)}\rho' U^{(l)\dagger} C^\dagger) = \frac{\mathbb{I}}{2^{Nn}}, \tag{22}$$

which follows from the privacy proof of the delegated measurements protocol outlined in Appendix B.

We show in Appendix C that our protocol achieves a soundness of $\delta = \frac{1}{N}$. Therefore, to maintain a similar level of precision in the cryptographic framework, we must have that

$$\frac{1}{\alpha N} \leqslant \frac{1}{\nu} \Rightarrow N \geqslant \frac{\nu}{\alpha}. \tag{23}$$

After ν repetitions of the prepare, encode, and measure part of the quantum metrology scheme, this translates to an additional

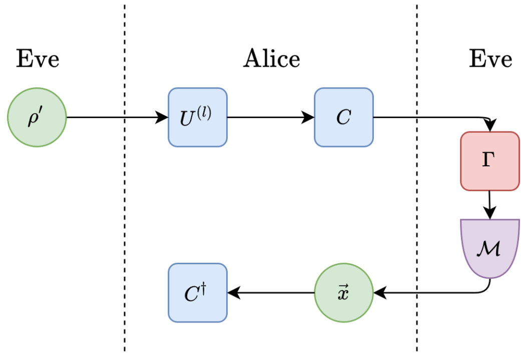

FIG. 3. Ideally, Eve provides Alice the quantum state $\rho^{\otimes N}$, but in principle Eve can send Alice any Nn qubit state ρ'. Upon receipt, Alice encodes the unknown parameter of the quantum metrology problem in the lth block of n qubits with $U^{(l)}$ and then encrypts the total quantum state with a Clifford C. All nonencoded blocks of qubits are then subjected to the verification protocol presented in [24], where Alice requests Eve for them to be measured with respect to the basis of an arbitrary (now encrypted) stabilizer of ρ. Again, without loss of generality, the measurement results $\vec{x} = x_1, \ldots, x_N$ returned by Eve can be interpreted as if Eve performed an attack Γ before performing the requested measurement $\mathcal{M}$. Alice accepts the measurement result if (after postprocessing) the measurement result of the nonencoded blocks each results in a $+1$ eigenvalue with respect to their respective stabilizer measurement.

$\mathcal{O}(\nu^2/\alpha)$ number of quantum states, or a quadratic increase compared to the ideal framework.

VI. DELEGATED PARAMETER ENCODING

The final scenario we consider is when the task of parameter estimation is delegated to an untrusted third party. From a verification perspective, the goal is to assure that some output state ρ_{out} is close to the ideal encoded state ρ_θ with high probability. Unsurprisingly, this is an impossible task from an information theoretic standpoint without having perfect knowledge of θ, which would entirely defeat the purpose of quantum metrology. The impossibility of this task stems from the fact that an adversary can manipulate the lack of information about θ to their advantage. For example, an adversary can introduce a slight bias $\Lambda_{\theta+\delta\theta}$, encode a different parameter altogether Λ_φ, encode θ into a different quantum state $\tilde{\rho}$, or do nothing at all $\mathbb{I}$. Furthermore, there is no way of guaranteeing that an adversary acts identically each round. To have security we must have some additional assumptions.

Suppose, for example, that the abilities of the adversary are greatly limited to applying either Λ_θ or the identity $\mathbb{I}$. If one has *a priori* knowledge that $\theta \approx \theta_0$, a loose *accept* criterion is for the estimate to be within some range of θ_0. This "protocol" can still be manipulated by an adversary if they learn the range of acceptance: $\mathbb{I}$ is applied a small number of times such that the expected estimate falls within the acceptance range despite the added bias.

Finally, if the adversary is further hindered by assuming that they cannot access any sort of classical information—such as an *a priori* approximation $\theta \approx \theta_0$, or the acceptance range of the aforementioned protocol—then one can continue on with the quantum metrology scheme. This is because in this specific setting, the effective encoding map is now the CPTP map:

$$\rho \to (1-p)\Lambda_\theta(\rho) + p\rho, \tag{24}$$

where p is the effective probability that the adversary does nothing, and hence applies Λ_θ with effective probability $1 - p$. Here, the metrology problem of estimating θ has evolved into the multiparameter problem [47] of estimating θ and p. However, in making these assumptions, we have ventured out of the realm of cryptographic quantum metrology and into a fusion of quantum channel tomography [48] and quantum metrology.

VII. DISCUSSION

In this paper we expanded upon the formulation of cryptographic quantum metrology [12] by exploring various scenarios where a portion of a quantum metrology task is delegated to an untrusted party. In order to assure a notion of integrity, i.e., the functionality of the underlying quantum metrology problem is the same, we incorporate appropriate cryptographic protocols. For the scenarios where either state preparation or measurements are delegated to an untrusted party, we showed that cryptographic framework can attain the same level of precision as the ideal framework with a quadratic increase in resources. However, for the delegated parameter encoding scenario, we argued against the existence of any information theoretic cryptography protocols which would permit this setting. This is because any such protocol would require perfect knowledge of θ, which defeats the purpose of quantum metrology.

The protocols established in this paper build upon existing cryptographic protocols, namely, quantum state verification [23], quantum message authentication [19], and blind quantum computing [43]. In principle one can incorporate other relevant cryptographic protocols, such as quantum process tomography [28,48], provided that the incorporation does not interfere with the parameter encoding. Similarly, one can incorporate protocols relevant to the specific nature of the malicious adversary; one may use a simpler protocol when dealing with honest-but-curious adversaries [16–18], or when dealing with specific attacks (e.g., covertness protocols, which have recently been adopted to quantum sensing [49,50]).

For the sake of continuity with [12], we used the soundness as a cryptographic figure of merit. Note, though, that in the specific case of delegated state preparation and incorporating verification protocols, there are several possible figures of merit which are intertwined [22,23]. For example, in this paper the soundness δ was bounded for a fixed N. However, the framework presented in [22,23] permits finding an N for a fixed δ and α. For example, for qubit stabilizer states (such as the GHZ state) the answer is $N = 2(\ln 2)^{-1}\delta^{-1}\ln\alpha^{-1}$ (see also [51]). The bounds are different because the "worst case" attack which saturates the soundness for a fixed N is different than the worst case attack for a fixed δ.

In any of the scenarios presented, one can eliminate the possibility of a multiround attack, i.e., a malicious attack correlated over a number of rounds, by realizing that we can equivalently formulate the problem of performing the protocol on one giant quantum state and achieve the same level of soundness with the same number of resources. For example, in the second scenario, if $\rho_{\text{in}} \to \rho_{\text{in}}^{\otimes \nu}$, then the same level of soundness is achieved since $n \to \nu n$ and $t \to \nu t$.

In this paper, as well as in [12], we restricted the quantum metrology problem to a single parameter estimation problem. However, as the cryptographic protocols do not affect the estimation strategy, one could consider multiparameter estimation problems [47]. However, the estimators used in multiparameter problems are more complex and thus the bounds on the bias, Eq. (14), and integrity, Eq. (15), do not necessarily hold. Generalizing these bounds to multiparameter estimators, and even other single parameter estimators, is a future perspective for cryptographic quantum metrology.

Quantum sensing networks have recently been proposed for a variety of applications, such as synchronizing clocks [15,46] and spatially distributed sensing problems [52–54]. Quantum networks [11,55] are a collection of nodes connected via quantum channels, and different nodes have access to different quantum technologies. The work presented in this paper easily integrates with quantum sensing networks to add a security aspect to the problem if one or more of the nodes are untrusted.

ACKNOWLEDGMENTS

We acknowledge fruitful discussions with Elham Kashefi and financial support from ANR Grant No. ANR-17-CE24-0035 VanQuTe.

APPENDIX A: METHODOLOGY ON BOUNDING THE SOUNDNESS

In the main text, the soundness was introduced as a bound on the quantity

$$\frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}} p_{\text{acc}}(k,\Gamma)\cdot[1-F(\rho_{\text{id}},\rho_{\text{out}}(k,\Gamma))], \tag{A1}$$

where $\rho_{\text{out}}(k,\Gamma)$ is the quantum state of the metrology qubits (for both protocols these are measurement statistics) conditional on the measurement results of the ancillary flag qubits resulting in *accept*, and ρ_{id} is the ideal quantum state (again measurement statistics) of the metrology qubits. This expression is introduced as it can be used to derive the integrity of the relevant quantum metrology problem, Eqs. (14) and (15); however, the fidelity of quantum states, F, is a highly nonlinear function and difficult to manipulate. Instead, we will show that the soundness can be bounded with respect to the trace of a relevant quantity (which is much simpler to manipulate).

We drop the explicit dependence on k and Γ for conciseness: $p_{\text{acc}}(k,\Gamma)\to p_{\text{acc}}$ and $\rho_{\text{out}}(k,\Gamma)\to\rho_{\text{out}}$. This section of the Appendix is used for both protocols presented in the main text, thus the formalism is quite general; nonetheless, the specific values will be provided for clarification. We reference the first protocol as DM (delegated measurements) and the second protocol as (DSM) (delegated state preparation and measurements).

In both protocols, after postprocessing the measurement result originates from the measurement statistics of

$$A^\dagger\mathcal{M}[\Gamma(A\rho_a A^\dagger)]A, \tag{A2}$$

where A is an encryption operation used by Alice (in DM $A\to C\pi$, in DSM $A\to C$), $\mathcal{M}$ is the measurement requested by Alice, and ρ_a is the quantum state in the possession of Alice before the encryption. In both protocols, the requested measurement is some ideal projective measurement $\mathcal{M}_{\text{id}}$ where the requested basis is altered with respect to the encryption A. Specifically, if $\mathcal{M}_{\text{id}}$ has projectors $\{E\}$ then $\mathcal{M}$ has projectors $\{AEA^\dagger\}$, thus

$$A^\dagger\mathcal{M}[\Gamma(A\rho_a A^\dagger)]A=\mathcal{M}_{\text{id}}[A^\dagger\Gamma(A\rho_a A^\dagger)A]=\mathcal{M}_{\text{id}}(\rho_f), \tag{A3}$$

where $\rho_f = A^\dagger\Gamma(A\rho_a A^\dagger)A$ is an effective final quantum state from which the measurement statistics are derived.

For the sake of clarity, we henceforth order $\mathcal{M}_{\text{id}}(\rho_f)$ by metrology qubits followed by the flag qubits. The measurement statistics $\mathcal{M}_{\text{id}}(\rho_f)$ can be expressed as a linear combination of quantum states which result in *accept* or *reject*:

$$\mathcal{M}_{\text{id}}(\rho_f)=p_{\text{acc}}\sum_\lambda \frac{p_\lambda}{p_{\text{acc}}}\rho_{\text{out},\lambda}\otimes|\lambda\rangle\langle\lambda| + (1-p_{\text{acc}})\rho_{\text{disc,rej}}, \tag{A4}$$

where $\{|\lambda\rangle\langle\lambda|\}$ is the set of measurement results (on the flag qubits) which are accepted by Alice, with a specific result $|\lambda\rangle\langle\lambda|$ occurring with probability p_λ (where $\sum_\lambda p_\lambda = p_{\text{acc}}$), $\rho_{\text{out},\lambda}$ is the measurement statistics of the metrology qubits if $|\lambda\rangle\langle\lambda|$ is observed, and $\rho_{\text{disc,rej}}$ is a combination of metrology qubits and flag qubits the form of which is irrelevant as the flag qubits result in *reject* and thus the measurement statistics of metrology qubits are discarded. In DM, the only measurement result which is accepted is $|0\rangle\langle 0|^{\otimes t}$; however, in DSM, the measurement result is accepted if the jth block of n qubits is a $+1$ eigenvalue of S_j for all $j\neq l$. Thus, if Alice accepts the measurement result, the measurement statistics used for quantum metrology is

$$\rho_{\text{out}}=\sum_\lambda \frac{p_\lambda}{p_{\text{acc}}}\rho_{\text{out},\lambda}. \tag{A5}$$

We denote the number of accepted $|\lambda\rangle\langle\lambda|$ as no. λ. If Alice sends Eve $\rho_\theta\otimes|\lambda\rangle\langle\lambda|$ (for any λ), and Eve acts honestly, then $\mathcal{M}_{\text{id}}(\rho_\theta\otimes|\lambda\rangle\langle\lambda|)=\rho_{\text{id}}\otimes|\lambda\rangle\langle\lambda|$. Using the concavity of the fidelity

$$\begin{aligned}
&\frac{1}{\text{no. }\lambda}\sum_\lambda F(\rho_\theta\otimes|\lambda\rangle\langle\lambda|,\rho_f)\\
&\leqslant \frac{1}{\text{no. }\lambda}\sum_\lambda F(\rho_{\text{id}}\otimes|\lambda\rangle\langle\lambda|,\mathcal{M}_{\text{id}}(\rho_f))\\
&\leqslant F\left(\frac{1}{\text{no. }\lambda}\sum_\lambda \rho_{\text{id}}\otimes|\lambda\rangle\langle\lambda|,\mathcal{M}_{\text{id}}(\rho_f)\right)\\
&= p_{\text{acc}}F\left(\frac{1}{\text{no. }\lambda}\sum_\lambda \rho_{\text{id}}\otimes|\lambda\rangle\langle\lambda|,\sum_\lambda\frac{p_\lambda}{p_{\text{acc}}}\rho_{\text{out},\lambda}\otimes|\lambda\rangle\langle\lambda|\right)\\
&= \frac{p_{\text{acc}}}{\text{no. }\lambda}F\left(\rho_{\text{id}},\sum_\lambda\frac{p_\lambda}{p_{\text{acc}}}\rho_{\text{out},\lambda}\right)\\
&= \frac{p_{\text{acc}}}{\text{no. }\lambda}F(\rho_{\text{id}},\rho_{\text{out}}).
\end{aligned} \tag{A6}$$

Assuming that ρ_θ is a pure state, then $F(\rho_\theta \otimes |\lambda\rangle\langle\lambda|, \rho_f) = \mathrm{Tr}(\rho_\theta \otimes |\lambda\rangle\langle\lambda|\rho_f)$. Because of the linearity of the trace, the summation over $|\lambda\rangle\langle\lambda|$ can be absorbed into the trace, from which it follows that

$$\mathrm{Tr}(\rho_\theta \otimes \Pi_{\mathrm{acc}}\rho_f) \leqslant p_{\mathrm{acc}} F(\rho_{\mathrm{id}}, \rho_{\mathrm{out}}), \tag{A7}$$

within the DM protocol

$$\Pi_{\mathrm{acc}}^{(\mathrm{DM})} = |0\rangle\langle 0|^{\otimes t}, \tag{A8}$$

and within the DSM protocol

$$\Pi_{\mathrm{acc}}^{(\mathrm{DSM})} = \bigotimes_{\substack{j=0\\ j\neq l}}^{N} \frac{\mathbb{I} + S_j}{2}. \tag{A9}$$

The probability of *accept* can also be computed via

$$p_{\mathrm{acc}} = \mathrm{Tr}[\mathbb{I} \otimes \Pi_{\mathrm{acc}}\mathcal{M}_{\mathrm{id}}(\rho_f)] = \mathrm{Tr}(\mathbb{I} \otimes \Pi_{\mathrm{acc}}\rho_f). \tag{A10}$$

Combining Eqs. (A6) and (A10), we obtain the inequality

$$\begin{aligned}\frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}} & p_{\mathrm{acc}} \cdot [1 - F(\rho_{\mathrm{id}}, \rho_{\mathrm{out}})] \\ &\leqslant \frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}} [\mathrm{Tr}(\mathbb{I} \otimes \Pi_{\mathrm{acc}}\rho_f) - \mathrm{Tr}(\rho_\theta \otimes \Pi_{\mathrm{acc}}\rho_f)] \\ &= \frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}} \mathrm{Tr}(\Pi\rho_f),\end{aligned} \tag{A11}$$

where $\Pi = (\mathbb{I} - \rho_\theta) \otimes \Pi_{\mathrm{acc}}$ projects the metrology qubits of ρ_f onto $\mathbb{I} - \rho_\theta$ and the flag qubits onto Π_{acc}. Recall that the quantum state was ordered by metrology qubits followed by flag qubits for simplicity in the derivation. The right-hand side of Eq. (A11) is much simpler to manipulate because of the linearity of the trace.

APPENDIX B: DELEGATED MEASUREMENTS TO AN UNTRUSTED PARTY

1. Privacy

The expected quantum state accessible to Eve is

$$\begin{aligned}\mathbb{E}(\tilde{\rho}) &= \frac{1}{\binom{m}{t}|\mathcal{C}_1|^m}\sum_{\pi}\sum_{C\in\mathcal{C}_1^{\otimes m}} C\pi\rho_{\mathrm{in}}\pi^{\dagger}C^{\dagger} \\ &= \frac{1}{\binom{m}{t}|\mathcal{C}_1|^m 2^m}\sum_{\pi}\sum_{C\in\mathcal{C}_1^{\otimes m}}\sum_{P\in\mathcal{P}_m} \mathrm{Tr}(P\pi\rho_{\mathrm{in}}\pi^{\dagger})CPC^{\dagger},\end{aligned} \tag{B1}$$

where $\mathcal{P}_m = \{\mathbb{I}, X, Y, Z\}^{\otimes m}$ is the mth Pauli group. Note that $\mathbb{I}$ is used to signify the identity map for any operator space, the dimension of which will be clear based on context. In the above equation, P and C can be constructed into m local operations. Recall that for any $Q \in \{X, Y, Z\}$ the set of local Clifford operations, $\mathcal{C}_1$, will map Q to a uniform distribution over $\{\pm X, \pm Y, \pm Z\}$. Therefore, unless P is uniquely equal to the identity map, the sum over $\mathcal{C}_1^{\otimes m}$ will result in zero. Thus, the summation can be simplified to

$$\mathbb{E}(\tilde{\rho}) = \frac{1}{\binom{m}{t}|\mathcal{C}_1|^m 2^m}\sum_{\pi}\sum_{C\in\mathcal{C}_1^{\otimes m}} \mathrm{Tr}(\pi\rho_{\mathrm{in}}\pi^{\dagger})C\mathbb{I}C^{\dagger} = \mathbb{I}/2^m. \tag{B2}$$

2. Local Clifford twirling

Before deriving a bound on the soundness of the protocol, we introduce a twirling lemma used in the protocol. The Clifford twirling lemma [56] states that for any m qubit quantum state ρ and $Q, R \in \mathcal{P}_m$ such that $Q \neq R$, then

$$\sum_{C\in\mathcal{C}_m} CQC^{\dagger}\rho CRC^{\dagger} = 0. \tag{B3}$$

As our protocol uses an arbitrary local Clifford, $C \in \mathcal{C}_1^{\otimes m}$, we show that a similar result holds. To understand why, we decompose ρ into a sum over the Pauli group

$$\begin{aligned}\sum_{C\in\mathcal{C}_1^{\otimes m}} & CQC^{\dagger}\rho CRC^{\dagger} \\ &= \frac{1}{2^m}\sum_{P\in\mathcal{P}_m}\sum_{C\in\mathcal{C}_1^{\otimes m}}\bigotimes_{j=1}^{m}(C_jQ_jC_j^{\dagger}P_jC_jR_jC_j^{\dagger}),\end{aligned} \tag{B4}$$

where the subscript j denotes that the operator acts on the jth qubit. Because each P_j can be expressed as a linear combination of quantum states, a corollary of the Pauli twirling lemma is that the above sum is zero if there exists a j such that $Q_j \neq R_j$. Hence if $Q \neq R$

$$\sum_{C\in\mathcal{C}_1^{\otimes m}} CQC^{\dagger}\rho CRC^{\dagger} = 0 \tag{B5}$$

3. Soundness

The soundness derivation presented here is identical to the one we present in [12]. The derivation begins by representing the attack Γ using a Kraus decomposition

$$\Gamma(\sigma) = \sum_{\alpha} A_\alpha \sigma A_\alpha^{\dagger}, \tag{B6}$$

which satisfies the completeness relationship $\sum_\alpha A_\alpha A_\alpha^{\dagger} = \mathbb{I}$. Each Kraus operator can be written as a sum over the Pauli operators

$$A_\alpha = \sum_{Q\in\mathcal{P}_m} a_{\alpha,Q}Q, \tag{B7}$$

where $a_{\alpha,Q} = 2^{-m}\mathrm{Tr}(QA_\alpha)$. Hence

$$\Gamma(\sigma) = \sum_{\alpha}\sum_{Q,R\in\mathcal{P}_m} a_{\alpha,Q}a_{\alpha,R}^{*}Q\sigma R, \tag{B8}$$

where an asterisk denotes the complex conjugate and the completeness relationship translates to

$$\sum_{\alpha}\sum_{Q,\mathcal{P}_m} |a_{\alpha,Q}|^2 = 1. \tag{B9}$$

Using this formulation, the expected final quantum state can be written as

$$\frac{1}{|\mathcal{K}|}\sum_{k\mathcal{K}}\rho_f = \frac{1}{\binom{m}{t}|\mathcal{C}_1|^m}\sum_{\pi}\sum_{C\in\mathcal{C}_1^{\otimes m}}\sum_{\alpha}\sum_{Q,R\in\mathcal{P}_m} a_{\alpha,Q}a^*_{\alpha,R}\pi^\dagger C^\dagger QC\pi\,\rho_{\text{in}}\pi^\dagger C^\dagger RC\pi, \tag{B10}$$

which is greatly simplified thanks to local Clifford twirling, Eq. (B5), which states that the only nonvanishing terms occur when $Q = R$:

$$\frac{1}{|\mathcal{K}|}\sum_{k\mathcal{K}}\rho_f = \frac{1}{\binom{m}{t}|\mathcal{C}_1|^m}\sum_{\pi}\sum_{C\in\mathcal{C}_1^{\otimes m}}\sum_{\alpha}\sum_{Q\in\mathcal{P}_m} |a_{\alpha,Q}|^2\pi^\dagger C^\dagger QC\pi\,\rho_{\text{in}}\pi^\dagger C^\dagger QC\pi. \tag{B11}$$

To more easily derive a bound on the soundness, we partition $\mathcal{P}_m$ into disjoint sets $\mathcal{P}_m^{(r)}$, with $0 \leqslant r \leqslant m$, where r signifies the number of nonidentity terms in a Pauli, for example $\mathbb{I}\otimes X \in \mathcal{P}_2^{(1)}$, hence

$$\frac{1}{|\mathcal{K}|}\sum_{k\mathcal{K}}\rho_f = \frac{1}{\binom{m}{t}|\mathcal{C}_1|^m}\sum_{\pi}\sum_{C\in\mathcal{C}_1^{\otimes m}}\sum_{\alpha}\sum_{r=0}^{m}\sum_{Q\in\mathcal{P}_m^{(r)}} |a_{\alpha,Q}|^2\pi^\dagger C^\dagger QC\pi\,\rho_{\text{in}}\pi^\dagger C^\dagger QC\pi. \tag{B12}$$

As per Eq. (A11), the soundness can be computed by projecting the above quantum state onto

$$\Pi = (\mathbb{I} - \rho_\theta)\otimes|0\rangle\langle 0|^{\otimes t}. \tag{B13}$$

There are $\binom{m-r}{t-s}$ choices of π such that $s \leqslant r$ of the nonidentity terms of $\pi^\dagger C^\dagger QC\pi \in \mathcal{P}_m^{(r)}$ interact with s of the flag qubits of Π (and thus $r - s$ nonidentity terms interact with the metrology qubits of Π). Recall that the Clifford group C_1 will map any $P \in \{X, Y, Z\}$ to an equal distribution over $\{\pm X, \pm Y, \pm Z\}$. The only nonvanishing terms occur when $C^\dagger$ maps these s terms exclusively onto $\pm Z$, which occurs for $3^{-s}|\mathcal{C}_1|^m$ of the local Cliffords. Finally, when $r \leqslant t$ and $s = r$ the trace similarly vanishes as the metrology qubits are completely unaffected. Define $s_{\max} = r - 1$ if $r \leqslant t$ and $s_{\max} = t$ otherwise. Using these simplifications, we obtain

$$\frac{1}{|\mathcal{K}|}\sum_{k\mathcal{K}}\text{Tr}(\Pi\rho_f) = \sum_{\alpha}\sum_{r=1}^{m}\sum_{Q\in\mathcal{P}_m^{(r)}}\sum_{s=0}^{s_{\max}} 3^{-s}|a_{\alpha,Q}|^2\frac{\binom{m-r}{t-s}}{\binom{m}{t}} \leqslant \sum_{r=1}^{m}\sum_{s=0}^{s_{\max}} 3^{-s}\frac{\binom{m-r}{t-s}}{\binom{m}{t}}, \tag{B14}$$

where the inequality follows from the completeness relationship, Eq. (B9). Rearranging the above sum

$$\begin{aligned}\frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}}\text{Tr}(\Pi\rho_f) &\leqslant \frac{1}{\binom{m}{t}}\sum_{s=0}^{t}3^{-s}\sum_{r=s+1}^{m}\frac{\binom{m-r}{t-s}}{\binom{m}{t}} = \sum_{s=0}^{t}3^{-s}\frac{\binom{m-s}{t-s+1}}{\binom{m}{t}} = \frac{m-t}{t+1}\sum_{s=0}^{t}3^{-s}\frac{(t+1)!(m-s)!}{(t-s+1)!m!}\\ &= \frac{m-t}{t+1} + \frac{m-t}{t+1}\sum_{s=1}^{t}3^{-s}\prod_{j=0}^{s-1}\frac{t+1-j}{m-j} \leqslant \frac{m-t}{t+1} + \frac{m-t}{t+1}\sum_{s=1}^{t}\left(\frac{t+1}{3m}\right)^s \leqslant \frac{3}{2}\frac{m-t}{t}.\end{aligned} \tag{B15}$$

APPENDIX C: DELEGATED STATE PREPARATION AND MEASUREMENTS TO AN UNTRUSTED PARTY

1. Effects of the Clifford encoding

Before deriving a bound on the soundness of the protocol, we first find a "closed form" expression of

$$S_Q = \frac{1}{|\mathcal{C}_1|^m}\sum_{C\in\mathcal{C}_1^{\otimes m}} CQC^\dagger\sigma CQC^\dagger, \tag{C1}$$

where σ is an m qubit quantum state and $Q \in \mathcal{P}_m$.

Define $\vec{x} \in \{0, 1\}^{\otimes}$ to be a vector of length m the entries of which correspond to the nonidentity terms of Q. Hence, if $\vec{x} = \{x_1, \dots, x_m\}$, then $x_j = 0$ if $Q_j = \mathbb{I}$ and $x_j = 1$ if $P_j \in \{X, Y, Z\}$. The magnitude of $\vec{x}$ is $x = \sum_j x_j$. We define a partial ordering $\vec{y} \preceq \vec{x}$ which satisfies $y_j \leqslant x_j\ \forall j$.

In the trivial case when $x = 0$, the corresponding P is the identity map and thus $S_Q = \sigma$. The general form is less trivial for $x = 1$, but the expression can still be simplified. Without loss of generality suppose $x_1 = 1$ (this is for conciseness, but it will be shown to be irrelevant). We begin by expanding σ over the Pauli basis:

$$S_Q = \frac{1}{2^m|\mathcal{C}_1|^m}\sum_{C\in\mathcal{C}_1^{\otimes m}}\sum_{P\in\mathcal{P}_m}\text{Tr}(P\sigma)\bigotimes_{j=1}^{m}C_jQ_jC_j^\dagger P_jC_jQ_jC_j^\dagger = \frac{1}{3\times 2^m}\sum_{R_1\in\mathcal{P}_1/\mathbb{I}}\sum_{P\in\mathcal{P}_m}\text{Tr}(P\sigma)R_1P_1R_1\bigotimes_{j=2}^{m}P_j, \tag{C2}$$

where the equality follows because the sum over the local Clifford group will map Q_1 onto an equal distribution of $\{\pm X, \pm Y, \pm Z\}$. We write that $\{X, Y, Z\} = \mathcal{P}_1/\mathbb{I}$. Equivalently, the above can be written as

$$\begin{aligned} S_Q &= \frac{1}{3\times 2^m}\left[\sum_{R_1\in\mathcal{P}_1}\sum_{P\in\mathcal{P}_m}\mathrm{Tr}(P\sigma)R_1P_1R_1\bigotimes_{j=2}^{m}P_j - \sum_{P\in\mathcal{P}_m}\mathrm{Tr}(P\sigma)P_1\bigotimes_{j=2}^{m}P_j\right] \\ &= \frac{4}{3\times 2^{m-1}}\sum_{P\in\mathcal{P}_{m-1}}\mathrm{Tr}(\mathbb{I}\otimes P\sigma)\frac{\mathbb{I}}{2}\otimes P - \frac{1}{3\times 2^m}\sum_{P\in\mathcal{P}_m}\mathrm{Tr}(P\sigma)P, \end{aligned} \tag{C3}$$

where equality arises because $P_1 \neq \mathbb{I}$ will commute with half of $\mathcal{P}_1$ and anticommute with the other half, thus resulting in a net sum of zero. The first sum is proportional to σ with a partial trace over the first qubit and replaced by the maximally mixed state $\mathbb{I}/2$. We define the notation $\mathrm{Tr}_{\vec{x}}\sigma$ to define the quantum state where all of the qubits indexed by $\vec{x}$ are traced out and replaced by the maximally mixed state $\mathbb{I}/2$. Therefore, $\sigma = \mathrm{Tr}_{\vec{0}}\sigma$, where $\vec{0}$ is the zero vector. Using this notation, we obtain that for $x = 1$

$$S_Q = \frac{4}{3}\mathrm{Tr}_{\vec{x}}\sigma - \frac{1}{3}\mathrm{Tr}_{\vec{0}}\sigma = \sum_{\vec{y}\preceq\vec{x}} c_{\vec{y}}\mathrm{Tr}_{\vec{y}}\sigma, \tag{C4}$$

where $c_{\vec{0}} = -1/3$ and $c_{\vec{x}} = 4/3$. As S_Q is a valid quantum state we have that $c_{\vec{0}} + c_{\vec{x}} = 1$. Even if the form was derived for $x_1 = 1$, the same form would have been obtained for all $\vec{x}$ with $x = 1$.

We will show using inductive reasoning that the form on the right-hand side of Eq. (C4) will hold true for any $Q' \in \mathcal{P}_m$. To do this, we first suppose that $Q' = QR_j$ where the nonidentity terms of Q' and Q are indexed by $\vec{x}'$ and $\vec{x}$, respectively, and $R_j \in \{X, Y, Z\}$ acts on the jth qubit and $x_j = 0$, thus $x' = x + 1$ and $x'_j = 1$. The inductive hypothesis is that S_Q can be expressed as

$$S_Q = \sum_{\vec{y}\preceq\vec{x}} c_{\vec{y}}\mathrm{Tr}_{\vec{y}}\sigma, \tag{C5}$$

with $\sum_{\vec{y}\preceq\vec{x}} c_{\vec{y}} = 1$. Because of the locality of the summation over the locally acting Clifford we have that

$$S_{Q'} = \frac{1}{|\mathcal{C}_1|^m}\sum_{C\in\mathcal{C}_1^{\otimes m}} CQ'C^\dagger\sigma CQ'C^\dagger = \frac{1}{|\mathcal{C}_1|}\sum_{C\in\mathcal{C}_1} CR_jC^\dagger S_Q CR_jC^\dagger = \sum_{\vec{y}\preceq\vec{x}} c_{\vec{y}}\left(\frac{1}{|\mathcal{C}_1|}\sum_{C\in\mathcal{C}_1} CR_jC^\dagger\mathrm{Tr}_{\vec{y}}\sigma CR_jC^\dagger\right). \tag{C6}$$

Since each $\mathrm{Tr}_{\vec{y}}\sigma$ is a quantum state, and R_j acts solely on the jth qubit, the $x = 1$ results can be used. Let us denote $\vec{y} + \delta_j$ as the vector with a 1 in the jth position as well as the same nonzero indices as $\vec{y}$; then

$$S_{Q'} = \sum_{\vec{y}\preceq\vec{x}} c_{\vec{y}}\left(\frac{4}{3}\mathrm{Tr}_{\vec{y}+\delta_j}\sigma - \frac{1}{3}\mathrm{Tr}_{\vec{y}}\right) = \sum_{\vec{y}'\preceq\vec{x}'} c_{\vec{y}'}\mathrm{Tr}_{\vec{y}'}\sigma, \tag{C7}$$

where $c_{\vec{y}'} = \frac{4}{3}c_{\vec{y}}$ if $\vec{y}' = \vec{y} + \delta_j$ for some $\vec{y} \preceq \vec{x}$, otherwise $\vec{y}' = \vec{y} \preceq \vec{x}$ and we set $c_{\vec{y}'} = -\frac{1}{3}c_{\vec{y}}$. It immediately follows that $\sum_{\vec{y}'\preceq\vec{x}'} c_{\vec{y}'} = 1$. Because the desired form of S_Q holds Q with $x = 1$, then this inductive argument will hold for any Q by continuously appending another nonidentity Pauli at the appropriate indices.

The reason we provide this derivation is to swap the order of the parameter encoding and the sum over local Clifford operations. In the protocol $m = Nn$ and a parameter is encoded on the lth block of n qubits via the unitary

$$U^{(l)} = \mathbb{I}^{\otimes n(l-1)} \otimes U_\theta^{\otimes n} \otimes \mathbb{I}^{\otimes n(N-l)}. \tag{C8}$$

It follows from the locality of $U^{(l)}$ that

$$\frac{1}{|\mathcal{C}_1|^m}\sum_{C\in\mathcal{C}_1^{\otimes m}} CQC^\dagger U^{(l)}\sigma U^{(l)\dagger}CQC^\dagger = \sum_{\vec{y}\preceq\vec{x}} c_{\vec{y}}\mathrm{Tr}_{\vec{y}}(U^{(l)}\sigma U^{(l)\dagger}) = \sum_{\vec{y}\preceq\vec{x}} c_{\vec{y}}U^{(l)}(\mathrm{Tr}_{\vec{y}}\sigma)U^{(l)\dagger} = U^{(l)}\left(\frac{1}{|\mathcal{C}_1|^m}\sum_{C\in\mathcal{C}_1^{\otimes m}} CQC^\dagger\sigma CQC^\dagger\right)U^{(l)\dagger}. \tag{C9}$$

2. Soundness

For the delegated state preparation protocol, the key k is a combination of three choices: which block of n qubits is encoded (l), the encryption operation (C), and the stabilizers $S_1, \ldots, S_{l-1}, S_{l+1}, \ldots, S_N$. For a specific key, the measurement statistics originate from

$$\rho_f = C^\dagger \Gamma(CU^{(l)}\rho' U^{(l)\dagger}C^\dagger)C = \sum_\alpha \sum_{Q\in\mathcal{P}_{Nn}} |a_{\alpha,Q}|^2 C^\dagger Q C U^{(l)}\rho' U^{(l)\dagger} C^\dagger Q C, \tag{C10}$$

where the CPTP map Γ was converted to a Pauli representation and simplified using the local Clifford twirling lemma Eq. (B5). As per Eq. (C9), the order of operators can be swapped:

$$\rho_f = \sum_\alpha \sum_{Q\in\mathcal{P}_{Nn}} |a_{\alpha,Q}|^2 U^{(l)} C^\dagger Q C \rho' C^\dagger Q C U^{(l)\dagger}. \tag{C11}$$

The soundness is a bound on the quantity

$$\frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}} \mathrm{Tr}(\Pi\rho_f) = \frac{1}{N|\mathcal{C}_1|^{Nn}|\mathcal{S}|^{N-1}} \sum_{l=1}^N \sum_{C\in\mathcal{C}_1^{\otimes Nn}} \sum_{S_1\in\mathcal{S}} \dots \sum_{S_{l-1}\in\mathcal{S}} \sum_{S_{l+1}\in\mathcal{S}} \dots \sum_{S_N\in\mathcal{S}} \mathrm{Tr}(\Pi\rho_f), \tag{C12}$$

where $\mathcal{S}$ is the set of stabilizers of ρ and

$$\Pi = U^{(l)}\left[\left(\frac{\mathbb{I}+S_1}{2}\right)\otimes\dots\otimes\left(\frac{\mathbb{I}+S_{l-1}}{2}\right)\otimes(\mathbb{I}-\rho)\otimes\left(\frac{\mathbb{I}+S_{l+1}}{2}\right)\otimes\dots\otimes\left(\frac{\mathbb{I}+S_N}{2}\right)\right]U^{(l)\dagger}. \tag{C13}$$

One of the restrictions introduced was that ρ is a stabilizer state (so that we could adopt the verification protocol constructed in [24]); stabilizer states exhibit many symmetries, one of which is

$$\frac{1}{|\mathcal{S}|}\sum_{S\in\mathcal{S}} S = \rho, \tag{C14}$$

hence

$$\frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}} \mathrm{Tr}(\Pi\rho_f) = \frac{1}{N|\mathcal{C}_1|^{Nn}} \sum_{l=1}^N \sum_{C\in\mathcal{C}_1^{\otimes Nn}} \mathrm{Tr}(U^{(l)}\bar{\Pi}_l U^{(l)\dagger}\rho_f) = \frac{1}{N|\mathcal{C}_1|^{Nn}} \sum_{l=1}^N \sum_{C\in\mathcal{C}_1^{\otimes Nn}} \sum_\alpha \sum_{Q\in\mathcal{P}_{Nn}} |a_{\alpha,Q}|^2 \mathrm{Tr}(\bar{\Pi}_l C^\dagger Q C\rho' C^\dagger Q C), \tag{C15}$$

where

$$\bar{\Pi}_l = \left(\frac{\mathbb{I}+\rho}{2}\right)^{\otimes(l-1)} \otimes (\mathbb{I}-\rho)\otimes \left(\frac{\mathbb{I}+\rho}{2}\right)^{\otimes(N-l)}. \tag{C16}$$

For any quantum state σ and projector P $\mathrm{Tr}(P\sigma)\leqslant \lambda_{\max}(P)$, where $\lambda_{\max}(P)$ is the largest eigenvalue of P. Using this fact, Eq. (C15) can be rearranged to obtain

$$\begin{aligned}\frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}} \mathrm{Tr}(\Pi\rho_f) &= \frac{1}{|\mathcal{C}_1|^{Nn}} \sum_{C\in\mathcal{C}_1^{\otimes Nn}} \sum_\alpha \sum_{Q\in\mathcal{P}_{Nn}} |a_{\alpha,Q}|^2 \mathrm{Tr}\left[C^\dagger Q C\left(\frac{1}{N}\sum_{l=1}^N \bar{\Pi}_l\right) C^\dagger Q C\rho'\right] \\ &\leqslant \frac{1}{|\mathcal{C}_1|^{Nn}} \sum_{C\in\mathcal{C}_1^{\otimes Nn}} \sum_\alpha \sum_{Q\in\mathcal{P}_{Nn}} |a_{\alpha,Q}|^2 \lambda_{\max}\left[C^\dagger Q C\left(\frac{1}{N}\sum_{l=1}^N \bar{\Pi}_l\right) C^\dagger Q C\right] \\ &= \frac{1}{|\mathcal{C}_1|^{Nn}} \sum_{C\in\mathcal{C}_1^{\otimes Nn}} \sum_\alpha \sum_{Q\in\mathcal{P}_{Nn}} |a_{\alpha,Q}|^2 \lambda_{\max}\left(\frac{1}{N}\sum_{l=1}^N \bar{\Pi}_l\right) \\ &= \lambda_{\max}\left(\frac{1}{N}\sum_{l=1}^N \bar{\Pi}_l\right).\end{aligned} \tag{C17}$$

This is much simpler to compute as each $\bar{\Pi}_l$ has the same eigenbasis: tensor products of either ρ or an orthogonal (pure state) $\tilde{\rho}$ (note that there are 2^n-1 different $\tilde{\rho}$, but interchanging them will not affect the eigenvalue). Consider the eigenvector of j copies of $\tilde{\rho}$ and $N-j$ copies of ρ. The only nonvanishing terms in the sum occur when the $\mathbb{I}-\rho$ term in $\bar{\Pi}_l$ interacts with a $\tilde{\rho}$ term in the eigenvector; the eigenvalue can be computed to be $\frac{j}{N2^{j-1}}$, thus

$$\frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}} \mathrm{Tr}(\Pi\rho_f) \leqslant \frac{1}{N}\cdot \max_{0\leqslant j\leqslant N}\frac{j}{2^{j-1}} = \frac{1}{N}. \tag{C18}$$

[1] V. Giovannetti, S. Lloyd, and L. Maccone, Advances in quantum metrology, Nat. Photonics **5**, 222 (2011).

[2] C. L. Degen, F. Reinhard, and P. Cappellaro, Quantum sensing, Rev. Mod. Phys. **89**, 035002 (2017).

[3] V. Giovannetti, S. Lloyd, and L. Maccone, Quantum-enhanced measurements: Beating the standard quantum limit, Science **306**, 1330 (2004).

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

[5] G. Tóth and I. Apellaniz, Quantum metrology from a quantum information science perspective, J. Phys. A: Math. Theor. **47**, 424006 (2014).

[6] C. M. Caves, Quantum-mechanical noise in an interferometer, Phys. Rev. D **23**, 1693 (1981).

[7] J. J. Bollinger, W. M. Itano, D. J. Wineland, and D. J. Heinzen, Optimal frequency measurements with maximally correlated states, Phys. Rev. A **54**, R4649 (1996).

[8] R. Krischek, C. Schwemmer, W. Wieczorek, H. Weinfurter, P. Hyllus, L. Pezzé, and A. Smerzi, Useful Multiparticle Entanglement and Sub-Shot-Noise Sensitivity in Experimental Phase Estimation, Phys. Rev. Lett. **107**, 080504 (2011).

[9] L. Pezzé and A. Smerzi, Quantum theory of phase estimation, arXiv:1411.5164.

[10] L. Pezze, A. Smerzi, M. K. Oberthaler, R. Schmied, and Philipp Treutlein, Quantum metrology with nonclassical states of atomic ensembles, Rev. Mod. Phys. **90**, 035005 (2018).

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

[12] N. Shettell, E. Kashefi, and D. Markham, Cryptographic approach to quantum metrology, Phys. Rev. A **105**, L010401 (2022).

[13] Z. Huang, C. Macchiavello, and L. Maccone, Cryptographic quantum metrology, Phys. Rev. A **99**, 022314 (2019).

[14] D. Xie, C. Xu, J. Chen, and A. M. Wang, High-dimensional cryptographic quantum parameter estimation, Quant. Info. Proc. **17**, 116 (2018).

[15] P. Kómár, 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).

[16] Y. Takeuchi, Y. Matsuzaki, K. Miyanishi, T. Sugiyama, and W. J. Munro, Quantum remote sensing with asymmetric information gain, Phys. Rev. A **99**, 022325 (2019).

[17] H. Okane, H. Hakoshima, Y. Takeuchi, Y. Seki, and Y. Matsuzaki, Quantum remote sensing under the effect of dephasing, Phys. Rev. A **104**, 062610 (2021).

[18] P. Yin, Y. Takeuchi, W.-H. Zhang, Z.-Q. Yin, Y. Matsuzaki, X.-X. Peng, X.-Y. Xu, J.-S. Xu, J.-S. Tang, Z.-Q. Zhou *et al.*, Experimental Demonstration of Secure Quantum Remote Sensing, Phys. Rev. Appl. **14**, 014065 (2020).

[19] H. Barnum, C. Crépeau, D. Gottesman, A. Smith, and A. Tapp, Authentication of quantum messages, in *The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002: Proceedings* (IEEE, New York, 2002), pp. 449–458.

[20] A. Broadbent and E. Wainewright, Efficient simulation for quantum message authentication, in *International Conference on Information Theoretic Security* (Springer, New York, 2016), pp. 72–91.

[21] Y. Takeuchi and T. Morimae, Verification of Many-Qubit States, Phys. Rev. X **8**, 021060 (2018).

[22] H. Zhu and M. Hayashi, Efficient Verification of Pure Quantum States in the Adversarial Scenario, Phys. Rev. Lett. **123**, 260504 (2019).

[23] H. Zhu and M. Hayashi, General framework for verifying pure quantum states in the adversarial scenario, Phys. Rev. A **100**, 062335 (2019).

[24] D. Markham and A. Krause, A simple protocol for certifying graph states and applications in quantum networks, Cryptography **4**, 3 (2020).

[25] A. Broadbent and C. Schaffner, Quantum cryptography beyond quantum key distribution, Des. Codes Cryptogr. **78**, 351 (2016).

[26] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, Darius Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani *et al.*, Advances in quantum cryptography, Adv. Opt. Photonics **12**, 1012 (2020).

[27] A. Gheorghiu, T. Kapourniotis, and E. Kashefi, Verification of quantum computation: An overview of existing approaches, Theory Comput. Syst. **63**, 715 (2019).

[28] Y.-C. Liu, J. Shang, X.-D. Yu, and X. Zhang, Efficient verification of quantum processes, Phys. Rev. A **101**, 042315 (2020).

[29] J. F. Fitzsimons and E. Kashefi, Unconditionally verifiable blind quantum computation, Phys. Rev. A **96**, 012303 (2017).

[30] Y. Takeuchi, A. Mantri, T. Morimae, A. Mizutani, and J. F. Fitzsimons, Resource-efficient verification of quantum computing using Serfling's bound, npj Quantum Inf. **5**, 27 (2019).

[31] C. A. Fuchs and J. Van De Graaf, Cryptographic distinguishability measures for quantum-mechanical states, IEEE Trans. Inf. Theory **45**, 1216 (1999).

[32] S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory* (Prentice-Hall, Englewood Cliffs, NJ, 1993).

[33] H. Cramér, Mathematical methods of statistics, in *Mathematical Methods of Statistics* (Princeton University Press, 1946).

[34] C. W. Helstrom, Quantum detection and estimation theory, J. Stat. Phys. **1**, 231 (1969).

[35] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (Springer, Holland, 1982).

[36] S. L. Braunstein and C. M. Caves, Statistical Distance and the Geometry of Quantum States, Phys. Rev. Lett. **72**, 3439 (1994).

[37] M. J. Holland and K. Burnett, Interferometric Detection of Optical Phase Shifts at the Heisenberg Limit, Phys. Rev. Lett. **71**, 1355 (1993).

[38] S. F. Huelga, C. Macchiavello, T. Pellizzari, A. K. Ekert, M. B. Plenio, and J. I. Cirac, Improvement of Frequency Standards with Quantum Entanglement, Phys. Rev. Lett. **79**, 3865 (1997).

[39] S. Pallister, N. Linden, and A. Montanaro, Optimal Verification of Entangled States with Local Measurements, Phys. Rev. Lett. **120**, 170502 (2018).

[40] Y.-C. Liu, X.-D. Yu, J. Shang, H. Zhu, and X. Zhang, Efficient Verification of Dicke States, Phys. Rev. Appl. **12**, 044020 (2019).

[41] N. Shettell and D. Markham, Graph States as a Resource for Quantum Metrology, Phys. Rev. Lett. **124**, 110502 (2020).

[42] D. Fattal, T. S. Cubitt, Y. Yamamoto, S. Bravyi, and I. L. Chuang, Entanglement in the stabilizer formalism, arXiv:quant-ph/0406168.

[43] A. Broadbent, J. Fitzsimons, and E. Kashefi, Universal blind quantum computation, in *2009 50th Annual IEEE Symposium on Foundations of Computer Science* (IEEE, New York, 2009), pp. 517–526.

[44] T. Morimae, Verification for measurement-only blind quantum computing, Phys. Rev. A **89**, 060302(R) (2014).

[45] D. Gottesman, The Heisenberg representation of quantum computers, arXiv:quant-ph/9807006.

[46] P. Kómár, T. Topcu, E. M. Kessler, A. Derevianko, V. Vuletić, J. Ye, and M. D. Lukin, Quantum Network of Atom Clocks: A Possible Implementation with Neutral Atoms, Phys. Rev. Lett. **117**, 060506 (2016).

[47] S. Ragy, M. Jarzyna, and R. Demkowicz-Dobrzański, Compatibility in multiparameter quantum metrology, Phys. Rev. A **94**, 052108 (2016).

[48] A. Bendersky, F. Pastawski, and J. P. Paz, Selective and Efficient Estimation of Parameters for Quantum Process Tomography, Phys. Rev. Lett. **100**, 190403 (2008).

[49] B. A. Bash, C. N. Gagatsos, A. Datta, and S. Guha, Fundamental limits of quantum-secure covert optical sensing, in *2017 IEEE International Symposium on Information Theory (ISIT)* (IEEE, New York, 2017), pp. 3210–3214.

[50] M. Tahmasbi and M. R. Bloch, On covert quantum sensing and the benefits of entanglement, IEEE Journal on Selected Areas in Information Theory **2**, 352 (2021).

[51] A. Unnikrishnan and D. Markham, Authenticated teleportation and verification in a noisy network, Phys. Rev. A **102**, 042401 (2020).

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

[53] 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).

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

[55] C. Simon, Towards a global quantum network, Nat. Photonics **11**, 678 (2017).

[56] C. Dankert, R. Cleve, J. Emerson, and E. Livine, Exact and approximate unitary 2-designs and their application to fidelity estimation, Phys. Rev. A **80**, 012304 (2009).