npj | quantum information

Article

Published in partnership with The University of New South Wales

https://doi.org/10.1038/s41534-025-01180-0

Faithful and secure distributed quantum sensing under general-coherent attacks

Check for updates

Gabriele Bizzarri[1], Marco Barbieri[1,2], Mylenne Manrique[1], Miranda Parisi[1], Fabio Bruni[1], Ilaria Gianani[1] & Matteo Rosati[3]

Quantum metrology and cryptography can be combined in a distributed and/or remote sensing setting, where distant end-users with limited quantum capabilities can employ quantum states, transmitted by a quantum-powerful provider via a quantum network, to perform quantum-enhanced parameter estimation in a private fashion. Previous works on the subject have been limited by restricted assumptions on the capabilities of a potential eavesdropper and the use of abort-based protocols that prevent a simple practical realization. Here we introduce, theoretically analyze, and experimentally demonstrate single- and two-way protocols for distributed sensing combining several unique and desirable features: (i) a safety-threshold mechanism that allows the protocol to proceed in low-noise cases and quantifying the potential tampering with respect to the ideal estimation procedure, effectively paving the way for wide-spread practical realizations; (ii) equivalence of entanglement-based and mutually-unbiased-bases-based formulations; (iii) robustness against collective attacks via a LOCC-de-Finetti theorem, for the first time to our knowledge. Finally, we demonstrate our protocols in a photonic-based implementation, observing that the possibility of guaranteeing a safety threshold may come at a significant price in terms of the estimation bias, potentially overestimating the effect of tampering in practical settings.

Quantum metrology enables the estimation of physical quantities with precision surpassing classical limits, thanks to the use of coherence and entanglement at the stages of probe preparation and measurement[1]. In recent years, advancements in the manipulation and transfer of quantum states over long distances, along with the vision of a fully connected quantum internet, have kindled the study of quantum metrology in a distributed and/or remote setting[2–23,23–25].

Distributed sensing is routinely used in current technologies as a way of monitoring systems, yielding information on their local and global properties as well[7–10]. This has prompted the investigation of its extension to quantum sensing[11]. Here, one or more distant parties aim to estimate some parameters using quantum states transmitted via a public quantum network, requiring considerations on the optimal distribution of resources[12,13]. It has been shown in an experiment that sharing entanglement among different partners estimating the average phase in their network is preferable to using local squeezing[15], followed by demonstrations with polarisation-entangled states[16,26]. In the same vein, adopting a network of atomic clocks linked by entanglement has been identified as a promising platform to realize a quantum-limited global positioning system[17].

Following on the integration of quantum metrology with communication, one is naturally led to consider the presence of malevolent agents in the network, being them in the form of eavesdroppers or untrusted nodes. Therefore, on top of the enhanced estimation capabilities provided by quantum sensors, one is typically interested in guaranteeing some notion of privacy with respect to other legitimate users and security against potential eavesdroppers. Such a scenario applies to a variety of practical settings for near- and mid-term quantum technologies, characterized by the presence of a fully quantum service-provider and an end-user client with limited quantum capabilities, e.g., the sensing of private medical data or of a natural phenomenon happening at a remote location.

In this article, we take a unifying approach to distributed quantum sensing (DQS), tackling the above-mentioned issues and providing experimental-friendly protocols for the estimation of a phase shift assisted by public quantum and classical communication. We present both a single-way protocol, where the probe remains in Bob's lab after phase-encoding, and a two-way protocol, where the probe is sent back to Alice for measurement, discussing how security cannot be guaranteed in the second case, while faithfulness is preserved. We note that our protocols can be equivalently formulated in terms of entanglement or mutually unbiased bases

[1]Dipartimento di Scienze, Università degli Studi Roma Tre, Rome, Italy. [2]Istituto Nazionale di Ottica, CNR, Florence, Italy. [3]Dipartimento di Ingegneria Civile, Informatica e delle Tecnologie Aeronautiche, Università degli Studi Roma Tre, Rome, Italy. e-mail: matteo.rosati@uniroma3.it

(MUBs), thus bridging previous approaches to the problem. Furthermore, for the first time to our knowledge, we prove that the protocols' properties are robust with respect to collective attacks by Eve, making use of a de Finetti theorem under single-way adaptive measurements due to ref. 27. Finally, we test our protocols via the implementation of optical-phase estimation using the photon polarization degree of freedom, providing evidence that the faithfulness can be guaranteed, in practice, only at the price of a potentially large bias on the estimated quantity.

Our effort builds on results that have appeared in the recent past. Restricting to the single-user setting, previous works have focused on the security requirement, relying on similar arguments to quantum key distribution (QKD): the experiment of ref. 2, based on the proposal in ref. 3, proposed an entanglement-based protocol, offering a secure link between two parties by means of a polarisation-entangled state, as in the scenario of Fig. 1. The integrity of the communication link has been verified by quantum state tomography, and, from the knowledge of the state, it has been possible to derive a fiducial statistical model for phase estimation. Crucially, this has shown a large asymmetry in the Fisher information available to the two parties and that potentially accessible to an eavesdropper. In addition, since the receiving party has no information on Alice's control, the protocol is also oblivious to Bob. In ref. 14, the authors considered the restricted case where the eavesdropper, Eve, is classical, and they can only intercept the measurement outcomes of the estimation procedure.

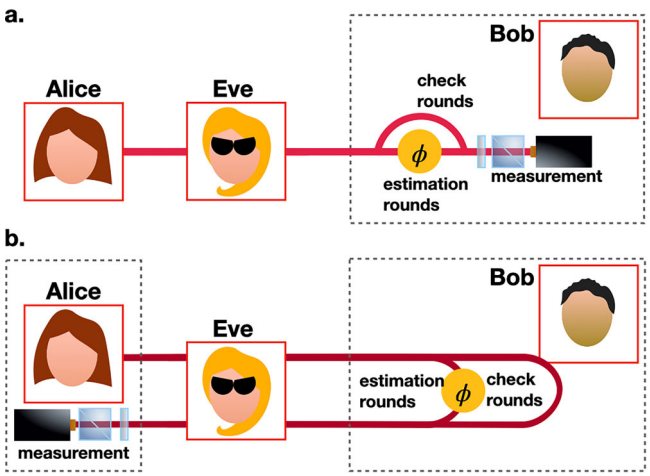


Fig. 1 | Depiction of the general DQS setting we consider. A provider Alice prepares quantum probe states and sends them to Bob, in order to estimate a parameter ϕ at a remote location. The transmission takes place on a quantum channel potentially controlled by a malicious adversary Eve, who can try to: (i) tamper with the probe in order to compromise the estimation; (ii) leak information in order to estimate the phase herself. **a** In the single-way setting, Bob can perform a quantum measurement at his location. **b** In the two-way setting, Bob is a passive party with no measurement capabilities, hence, the quantum state has to travel back to Alice after the parameter-encoding stage.

The work[4] has extended this protocol by relaxing the requirement of utilising an entangled state. This can be replaced with random separable states sent by Alice. Its experimental realisation in ref. 18 has shown the same asymmetry in Fisher information, with a setup compatible with quantum communication standards. In our article, we show that these two kinds of protocols are equivalent. Furthermore, rather than studying the estimation performance of Eve and Alice in a controlled scenario, we demonstrate Alice's capability of quantifying how much Eve has modified the quantum probe, and therefore setting up a safety threshold for aborting the protocol.

The general setting, instead, was studied in refs. 5,6, where the authors introduced single- and two-way estimation protocols between two legitimate users Alice and Bob, that communicate through quantum and classical channels controlled by Eve. In particular, ref. 5 has introduced fully cryptographic methods in quantum estimation with qubits, shortly followed by a generalisation to high-dimensional systems in ref. 19. The basic idea consists in extending the set of probe states to include decoy events along those that effectively estimate the parameter. This work has introduced the distinction between one-way protocols, in which Bob performs the measurement as well as imparting the parameter, and two-way protocols, in which Bob finally sends his state back to Alice following some possible information scrambling. This cryptographic approach has then been extended in ref. 6, enlarging the class of attacks to which the original proposal[5] is resilient. This comes at the cost of considering a large joint state of probe and flag states, which are then encrypted by means of code, in the form of Clifford operations, either collective or separable. This work has also the merit of introducing clear definitions for privacy, soundness, and integrity. However, a key limiting factor towards the implementation of these general protocols is that security can be enforced only at the cost of aborting the estimation procedure as soon as an error is detected, a procedure that we call abort-based. This is achieved by sending decoy or flag states on the quantum channel, and detecting whether they have been altered after transmission; in practice, such a zero-tolerance policy can lead to aborting the protocol at every round due to inevitable experimental errors, such as imperfect measurements or dark counts. Finally, the security of the above protocols has been analyzed only under the specific assumption of individual attacks by Eve, which, as in QKD, leaves it open to attacks that employ a quantum memory to establish quantum correlations between probes transmitted during subsequent uses of the channel.

An interesting application has been presented in ref. 22, followed by its experimental realisation in ref. 20. This scenario considers the estimation of a global phase parameter in a network, preventing information leakage about the local phase at the individual nodes. The notion of privacy in such quantum sensor networks has been elaborated in ref. 21. Here, we restrict to a single-provider/single-user setting, but we expect that our methods can be extended to the multi-user scenario. A summary of and a comparison with previous works related with our results on single-user DQS is provided in Table 1.

Table 1 | Comparison of different single-user DQS protocols in the literature with the ones proposed in this article

DQS Protocol	Quantum communication	Attacks	Security	Faithfulness	Entanglement-based
Protocol 1	1- & 2-way	General-coherent	Perfect (1w), None (2w)	Threshold-based	Yes
Protocol 2	1- & 2-way	General-coherent	Perfect (1w), None (2w)	Threshold-based	No
2,3	1-way	Classical	Perfect	A posteriori	Yes
4,18	1-way	Individual	Perfect	A posteriori	No
5	1- & 2-way	Individual	Perfect (1w), None (2w)	Abort-based	No
22	1- & 2-way	Individual	Perfect (1w), Zero-tolerance (2w)	Abort-based	No (trap code), Yes (Clifford code)

Attacks are labelled according to the capabilities of the eavesdropper (Eve); the security is deemed perfect whenever Eve holds a phase-independent completely mixed state, while it is zero-tolerance when based on passing a check. The faithfulness is labelled threshold-based when there is a safety margin for errors detected during the protocol, while it is abort-based when the margin is zero; instead, protocols working a posteriori require a complete tomographic analysis of the received state.

In our article, we strive to keep the protocol simple in terms of state-space dimension, while enlarging the class of attacks to the most general one allowed in QKD, i.e., where Eve can perform collective operations across different rounds of the protocol. This requires a significant extension of the theoretical methods introduced in the literature. For this purpose, the protocols are analyzed under the following specific requirements: *Faithfulness*–The legitimate users can estimate how much Eve has tampered with the ideal probe state, and hence quantify how much the actual estimation bias and error deviate from the ideal ones. Note that this is a combination of soundness and integrity as defined by ref. 6; *Security*–The legitimate users can quantify how much information about the estimated parameter has leaked to Eve.

Results

Theoretical framework and DQS protocol

Our DQS setting is shown in Fig. 1: a provider Alice with fully quantum capabilities can exchange quantum states $|\psi\rangle$ on a quantum channel with a technologically-limited party Bob, placed at a remote sensing location where a parameter ϕ can be encoded via a unitary operation $U(\phi)$. Bob's capabilities can range from a semi-passive switch, which essentially turns on or off to determine when the phase gets encoded, and then simply sends the probe quantum state back to Alice, to a quantum-classical sensor that can perform a destructive measurement of the probe and announce the outcome to Alice via a classical channel. Any kind of classical or quantum communication is assumed to be public, and hence controlled by a malicious adversary, Eve, with two distinct aims:*Tampering attack*–disrupting the estimation procedure by modifying the states transmitted on the quantum channel; *Leaking attack*–extracting information about the estimation procedure, in order to estimate the value of the parameter.

The performance of the protocol is measured in response to these two kinds of attacks, as defined below. *Faithfulness* quantifies the resilience to tampering attacks, and it can be measured by the distance of the ideal state from the tampered state after phase encoding, which bounds the estimation quality[6]:

Definition 1. (Faithfulness) A DQS protocol is ϵ-faithful if, when proceeding to estimation, it guarantees that the true phase-encoded state is ϵ-distant from the ideal phase-encoded state for a suitable distance measure.

Instead, *security* quantifies the resilience to leaking attacks, and it can be measured by the distance of Eve's share of the quantum state from the maximally mixed one, which allows no estimation at all:

Definition 2. (Security) A DQS protocol is ϵ-secure if, at any point, Eve's state is ϵ-distant from the completely mixed state, for a suitable distance measure.

At variance with previous works on the subject[5,6], we make no assumptions on Eve's capabilities, hence include the possibility to entangle the transmitted probe states with ancillary ones across multiple repetitions of the protocols and store the ancillae in a quantum memory for later collective quantum processing; this is the largest possible set of causal attacks by a quantum adversary, called general-coherent (GC) attacks in QKD[28].

In the following, without loss of generality, we assume that the probe state is that of an n-qubit system, and the parameter-encoding unitary is of the form $U(\phi)^{\otimes n}$ with $U(\phi) = e^{i\phi Y}$, with $Y = |R\rangle\langle R| - |L\rangle\langle L|$ the second Pauli matrix, $|R/L\rangle = (|0\rangle \pm i|1\rangle)/\sqrt{2}$ in the computational basis, and ϕ the phase to be estimated. It is well-known that optimal probes for estimating ϕ are the states

$$|\mathbf{0}/\mathbf{1}\rangle = \frac{|\mathbf{R}\rangle \pm |\mathbf{L}\rangle}{\sqrt{2}} \tag{1}$$

$$|+/-\rangle = \frac{|\mathbf{R}\rangle \pm i|\mathbf{L}\rangle}{\sqrt{2}}, \tag{2}$$

where $|\mathbf{R}/\mathbf{L}\rangle = |R/L\rangle^{\otimes n}$, yielding a factor-of-$n$ reduction in the variance with respect to a product state[1]. For later use, we indicate with bold symbols $\mathbf{X}, \mathbf{Y}, \mathbf{Z}$ the equivalent of Pauli matrices in the subspace span$\{|\mathbf{R}\rangle, |\mathbf{L}\rangle\}$ of the n-qubit space, i.e., those with eigenstates respectively (2), $|\mathbf{R}/\mathbf{L}\rangle$, and (1), in order to distinguish them from the ordinary Pauli matrices X, Y, Z. The fidelity between two quantum states is $F(\rho,\sigma) = ||\sqrt{\rho}\sqrt{\sigma}||_1^2$, while the trace-distance is $D(\rho,\sigma) = \frac{1}{2}||\rho - \sigma||_1$, with $||\cdot||_1$ the Schatten 1-norm; when ρ and/or σ are pure states, we indicate them with the corresponding ket in the arguments of these functions. We indicate with $||\cdot||_\infty$ the operator norm. Where explicitly stated, $\mathcal{D}(\mathcal{H})$ is the space of density matrices on the Hilbert space $\mathcal{H}$. For a state $\rho \in \mathcal{D}(\mathcal{H}^{\otimes(n+m)})$, we indicate as $\mathrm{Tr}_m[\rho] \in \mathcal{D}(\mathcal{H})$ the reduced state obtained by tracing out m parties.

Protocol 1. **One-way entanglement-based DQS**

1. *Preparation*: Alice prepares the entangled state
$$|\psi_+\rangle_{AB} = \frac{|0\rangle_A|+\rangle_B + |1\rangle_A|-\rangle_B}{\sqrt{2}}, \tag{3}$$
where A is a single-qubit and B is an n-qubit system. She then sends the B register to Bob via the quantum channel.
2. *Encoding*: Bob chooses to perform one of these three actions at random:
   (a) with probability p_c he does not encode the phase;
   (b) with probability p_e, he encodes the phase by applying $U(\phi)$ to the received state;
   (c) with probability $p_d = 1 - p_c - p_e$, he discards the received state and moves on to the next round of the protocol.
3. *Measurement*: Alice measures one of the observables X, Y, Z chosen uniformly at random. Bob performs one of these two actions, depending on what he did at step 2:
   (a) if he did not encode the phase, he measures one of the observables $\mathbf{X}$, $\mathbf{Y}$, $\mathbf{Z}$, chosen uniformly at random;
   (b) if he encoded the phase, then he measures one of the observables $\mathbf{X}$, $\mathbf{Z}$, chosen uniformly at random;
4. *Reconciliation and sifting*: After T repetitions of steps 1-3, Alice communicates to Bob the observables she measured in each round and the corresponding outcomes. Bob then keeps all rounds in which the following products of observables were measured, discarding the others:
   (a) $X_A \otimes \mathbf{Z}_B$, $Z_A \otimes \mathbf{X}_B$, and $Y_A \otimes \mathbf{Y}_B$, if he did not encode the phase;
   (b) $X_A \otimes \mathbf{Z}_B$ and $Z_A \otimes \mathbf{X}_B$, if he encoded the phase.
5. *Fidelity check*: From the sifted rounds (a) where he did not encode the phase, Bob estimates the fidelity of the received state with the ideal state $|\psi_+\rangle$ as follows:
$$\widehat{F} = \frac{1 + \langle X\otimes\mathbf{Z}\rangle + \langle Z\otimes\mathbf{X}\rangle + \langle Y\otimes\mathbf{Y}\rangle}{4}, \tag{4}$$
where the expectation is taken with respect to the tampered state. If $\widehat{F} \geq 1 - \epsilon^2$, for a given safety threshold ϵ, then Bob proceeds to the next step 6. Otherwise, he aborts the protocol.
6. *Phase estimation*: From the sifted rounds (b) where he applied $U(\phi)$, Bob estimates the phase as
$$\frac{1}{2}\arccos\left(\frac{\langle X\otimes\mathbf{Z}\rangle + \langle Z\otimes\mathbf{X}\rangle}{2}\right), \tag{5}$$
where the expectation is taken with respect to the phase-encoded tampered state.

The main protocol that we will consider is described in Protocol 1. It relies on shared entanglement between the provider, Alice, and the end-user, Bob; the latter is also required to randomize its actions during several rounds, in order to guarantee security agasinst GC attacks from Eve. Furthermore, it is formulated directly in terms of measurements of Pauli-like observables to facilitate experimental realization. Indeed, while Alice keeps a single qubit in her lab, she can send an n-qubit probe state to Bob to achieve quantum-enhanced estimation performance. Nevertheless, Bob only needs

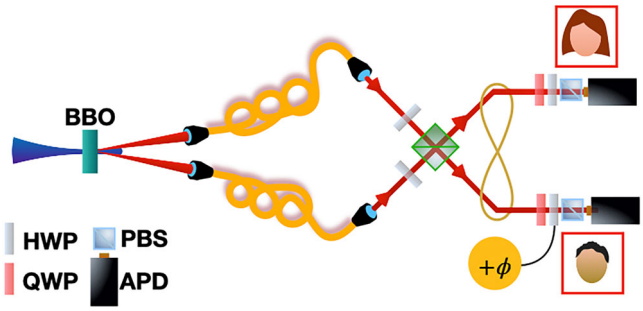


Fig. 2 | Sketch of the experimental setup: photon pairs generated by SPDC process in a BBO crystal are sent via single-mode optical fibers into a control-Z gate. After the two photons are entangled, their polarization is measured. Here, on estimation rounds, the target phase ϕ is imparted on one arm. Detected photons are then delivered to avalanche photodiodes (APDs) single photon detectors via single-mode optical fibers.

to measure two-dimensional observables on the n-qubit space. We note that an equivalent scheme can be formulated that does not rely on shared entanglement, but rather MUBs (Protocol 2). While from a theoretical perspective, the two protocols elucidate different aspects of the security guarantee, the choice of implementing one or the other might depend on experimental constraints and available resources.

Note that steps 5–7 can also work in a reverse-reconciliation fashion, i.e., with Bob announcing his measurements, outcomes and check/estimation rounds to Alice, since Eve does not have access to the observables measured by Alice in each round. However, security would be immediately compromised in that case, unless Bob first announces the results of check rounds and, once the check is passed and they are sure that Eve has meddled little with the probe, he announces the results of the estimation rounds.

The core of the protocol is in the alternation of different rounds on Bob's side: check rounds where the phase is not encoded are used to detect and quantify the presence of Eve in the channel; estimation rounds are actually used for phase-estimation; discard rounds are employed to guarantee security against GC attacks, as in QKD. The parameters p_e, p_c and p_d, together with the measurements' randomization, determine the fraction of check, estimation and discarded rounds after sifting: for large T, we expect to obtain $N_c \simeq p_e T/3$ sifted check rounds and $N_e \simeq p_c T/3$ sifted estimation rounds, while approximately $N_d \simeq p_d T + (1-p_d)2T/3 = (2+p_d)T/3$ rounds are discarded. These latter rounds are need to ensure that the protocol is robust to GC attacks, satisfying the requirement $N_d \gg N_e + N_c$ via the choice of a suitable $p_d \gg 0$. If, instead, one restricts to individual attacks, it is sufficient to take $p_d = 0$.

Furthermore, note that Protocol 1 can be easily extended to a two-way framework, wherein Bob takes on a more passive role: in step 3, he can only decide between actions (a) or (b), after which he sends the n-qubit quantum state back to Alice via the quantum channel. The subsequent steps are then all carried out by Alice in her lab, including case (c), i.e., discarding a fraction p_d of the received states. Unfortunately, in this case, only faithfulness can be guaranteed, while security is rendered impossible by Eve's interaction with the probe before and after phase-encoding, which can potentially give her full access to the phase information without Alice noticing. Similar observations in ref. 6 led the authors to devise an encryption-decryption mechanism for Bob's phase-encoding, which significantly complicates the protocol, yielding itself to a large abortion rate in practical noisy scenarios.

The faithfulness and security guarantees of our proposed protocol are provided in the following Theorem:

Theorem 1. The one-way entanglement-based DQS Protocol 1 is perfectly secure and its faithfulness is determined by ϵ. Indeed, the difference of bias and variance of an unbiased estimator $\widehat{\phi}$ calculated on the ideal probe state with respect to the same estimator $\widehat{\phi}'$ on the tampered state are bounded, under GC attacks, as

$$\left|\mathbb{E}\widehat{\phi} - \mathbb{E}\widehat{\phi}'\right| \leq \frac{\epsilon_0}{n|\sin(2n\phi)|}, \tag{6}$$

$$\left|\Delta^2\widehat{\phi} - \Delta^2\widehat{\phi}'\right| \leq \frac{(2\epsilon_0 + \epsilon_0^2)}{n^2\sin^2(2n\phi)}. \tag{7}$$

with $\epsilon_0 = \sqrt{\frac{2}{3}\epsilon^2 + 4f\left(T, N_d, n\right)}$ and $f(T,x,n) = (T-x-1)\sqrt{\frac{n}{2x}}$. In the case of individual attacks, one can take $N_d = 0$ and employ the same bias bound of (6) with $\epsilon_0 \mapsto \sqrt{\frac{2}{3}}\epsilon$, while the variance bound reads

$$\left|\Delta^2\widehat{\phi} - \Delta^2\widehat{\phi}'\right| \leq \frac{(2\epsilon_0/N_e + \epsilon_0^2)}{n^2\sin^2(2n\phi)}. \tag{8}$$

The two-way version of the protocol has similar bounds with $\epsilon_0 \mapsto \sqrt{\frac{2}{3}\epsilon^2 + 4f\left(T, N_d, n\right)} + |\sin(\min\{n\phi, \pi/2\})|$.

The proof of Theorem 1, deferred to "Methods", relies on three main steps: (i) showing the equivalence of Protocol 1 to a MUB-based protocol where Alice sends as probe state the eigenstate of a random Pauli matrix and Bob applies corresponding measurements during the check and estimation rounds; (ii) showing that, even in the presence of GC attacks, the fidelity measured during check rounds quantifies equally well the fidelity to the phase-encoded state used in the estimation rounds, via a suitable de-Finetti theorem; (iii) correcting the bias and variance estimates accordingly.

Experimental implementation and results

Protocol 1 was tested at the proof-of-principle stage. We did not aim at reproducing all features of a complete implementation, but rather to obtain experimental data compatible with it, choosing $p_e = p_c = 1/2$ and $p_d = 0$, thus addressing individual attacks. For this purpose, we employed photonic qubits with polarisation encoding by means of the setup presented in Fig. 2. A photon pair is produced by spontaneous parametric down-conversion, and delivered on a photonic control-Z gate in order to generate a state close to maximal entanglement - this corresponds to setting $n = 1$ in Alice and Bob's shared resource Eq. (3).

Polarisation measurements, associated to Pauli operators, are carried out as customary, by means of waveplate and polarisers. During the check rounds, the correlators $\langle X \otimes Z\rangle, \langle Z \otimes X\rangle, \langle Y \otimes Y\rangle$ are reconstructed, leading to a fidelity $F = 0.937 \pm 0.017$ ($\epsilon = 0.251 \pm 0.034$), calculated according to (4). We attribute all of the discrepancy to the tampering action of Eve, even if we do not perform attacks actively. As for the estimation rounds, the phase is encoded not by means of an additional object, but by an additional rotation of Bob's plate by an angle θ—this corresponds to a phase $\phi = 2\theta$. The estimator (5) valid for the ideal state has been employed: its bias (6) and discrepancy for the variance (7) have then been studied as a function of θ. The results are presented in Figs. 3 and 4.

From Fig. 3, we observe that the impact of tampering on phase estimation is more pronounced for small values of ϕ. However, this is not reflected in the variance, which shows a scattered profile in proximity of the ideal Cramér-Rao limit. Instead, Fig. 4 clearly shows that the deviation of bias and variance predicted theoretically from Theorem 1 tends to significantly overestimate the real ones.

In order to assess our results against typical attacks, we have performed analytical calculations based on specific noise models for the communication channel. The resulting differences in bias and variance distortion are shown in Figs. 5 and 6, showing the case of a dephasing channel and a depolarising channel, respectively. The former captures qualitatively what has been observed in the data. We also remark how a tampering attack based on depolarisation leads to an expected discrepancy of the variance, which is identically zero, even if a bias is present (except for the limiting case of complete depolarisation that shows vanishing Fisher information).

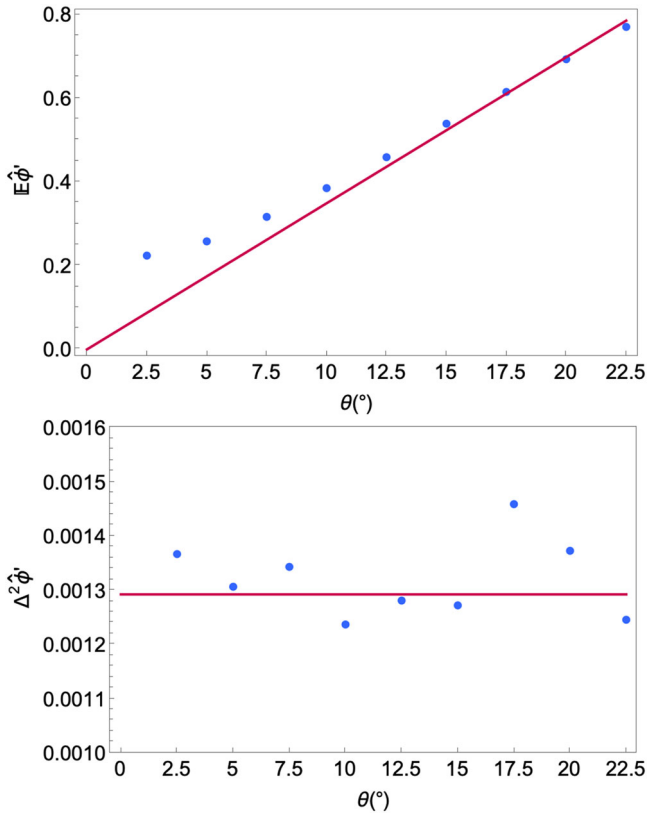


Fig. 3 | Results of the phase estimation. Top: retrieved value $\mathbb{E}\widehat{\phi'}$ (blue points) as a function of the plate setting θ, compared with the expectation $\phi' = 2\theta$ (solid red curve). Bottom: experimental value $\Delta^2\widehat{\phi'}$ (blue points), compared with the Cramér-Rao bound for the ideal maximally entangled state (solid red curve).

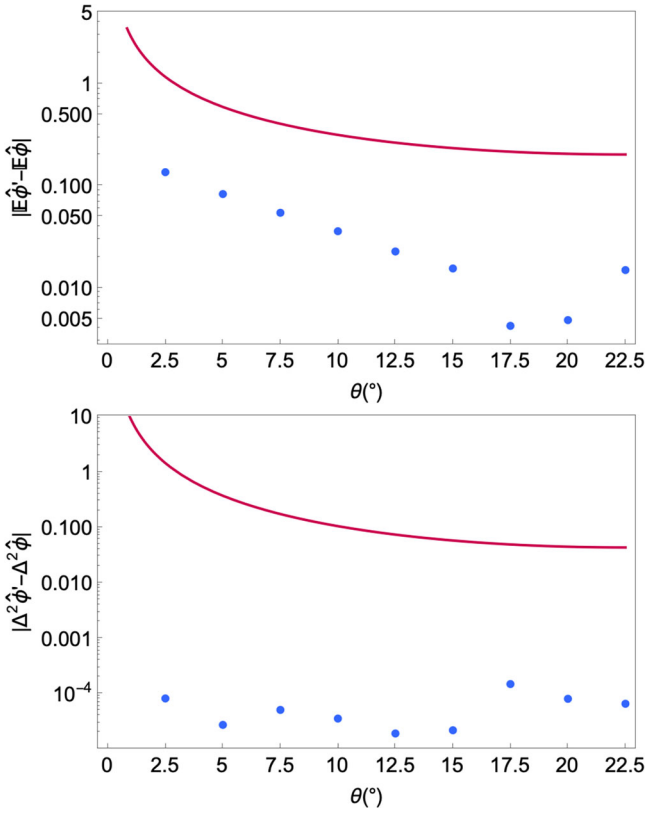


Fig. 4 | Precision of phase estimation. Top: bias with respect to the ideal case (blue points), compared with the bound (6) calculated based on the experimental fidelity (red solid line). Bottom: discrepancy from the ideal case (blue points), compared with the bound (7) calculated based on the experimental fidelity and the available events (red solid line).

This confirms the relevance of implementing fidelity checks, as purely metrological considerations might exhibit limited sensitivity to attacks.

Discussion

In this article, we have proposed a DQS protocol with several desirable features, including: (i) practical security criterion via a threshold-based approach; (ii) faithfulness of the estimation guaranteed against the largest class of collective quantum attacks, i.e., GC attacks; (iii) ease of implementation with minimal resources, via bipartite entangled states or mutually unbiased bases. Our work tackles multiple issues raised in previous works, providing a unified information-theoretic perspective on remote sensing with cryptographic guarantees. We expect that our methods will be applicable to the multi-user scenario, complementing the purely metrological approach of the literature[21,22,29], as well as to continuous-variable quantum systems where the combination of communication and sensing problems is common[30–34].

From a practical perspective, our results highlight that the bound on bias and variance with respect to the ideal estimation can significantly overestimate Eve's effective tampering; we attribute this overestimation to the use of trace-distance, which can be easily employed to bound the deviation of bias and variance in theory, while it must be estimated via the fidelity in practice. On one hand, this leaves open the possibility of finding more refined bounds that take into account the actual observable being measured, seeking to employ the measured fidelity directly. On the other hand, we cannot exclude that, without acquiring more specific information on the transmitted probe state, the quantification of metrological performance exclusively via cryptographic parameters (e.g., faithfulness) is fundamentally limited. Future works on the subject should address this conundrum.

Finally, tackling the tradeoff between security, faithfulness, and the protocol's complexity for guaranteeing them might require a thoughtful and accurate characterization of Bob's technological capabilities, also accounting for the distributed and/or remote problem setting. For example, in order to ensure security in the two-way scenario, it might be strictly necessary to require that Bob can create entanglement, such as in ref. 6, potentially rendering remote state generation unnecessary. It remains an open question whether other strategies, based on lesser technological demands on Bob's side, might still grant security. Another interesting direction to investigate is restricting Eve's capabilities, e.g., in the two-way scenario, one can expect to obtain security if Eve is prevented from intercept-resend attacks.

Methods

Faithfulness proof for the one-way protocol

The first step towards proving Theorem 1 is reducing it to a MUB-based protocol that randomizes the state sent to Bob. Let $\mathbf{P} \in \{\pm\mathbf{X}, \pm\mathbf{Y}, \pm\mathbf{Z}\}$ be a Pauli-like observable, $|\mathbf{P}, \pm\rangle$ its ±1-eigenvectors, and consider the MUB-based Protocol 2. This protocol does not require entanglement and its equivalence to Protocol 1 can be easily shown, since each measurement on Alice's side in the latter determines an instance of the randomly chosen observable $\mathbf{P}$ in the former:

Lemma 1. Protocols 1 and 2 are equivalent, up to a rescaling of the safety threshold $\epsilon^2 = 3\bar{\epsilon}^2/2$.

Proof. In the entanglement-based protocol, Alice's register never interacts with Eve, hence the expectations in (4) can be expressed as follows:

$$\langle Z \otimes \mathbf{X}\rangle = \frac{\mathrm{Tr}[\mathbf{Z}\cdot\Phi(|+\rangle\langle+|)] - \mathrm{Tr}[\mathbf{Z}\cdot\Phi(|-\rangle\langle-|)]}{2}, \tag{9}$$

$$\langle X \otimes \mathbf{Z}\rangle = \frac{\mathrm{Tr}[\mathbf{X}\cdot\Phi(|\mathbf{0}\rangle\langle\mathbf{0}|)] - \mathrm{Tr}[\mathbf{X}\cdot\Phi(|\mathbf{1}\rangle\langle\mathbf{1}|)]}{2}, \tag{10}$$

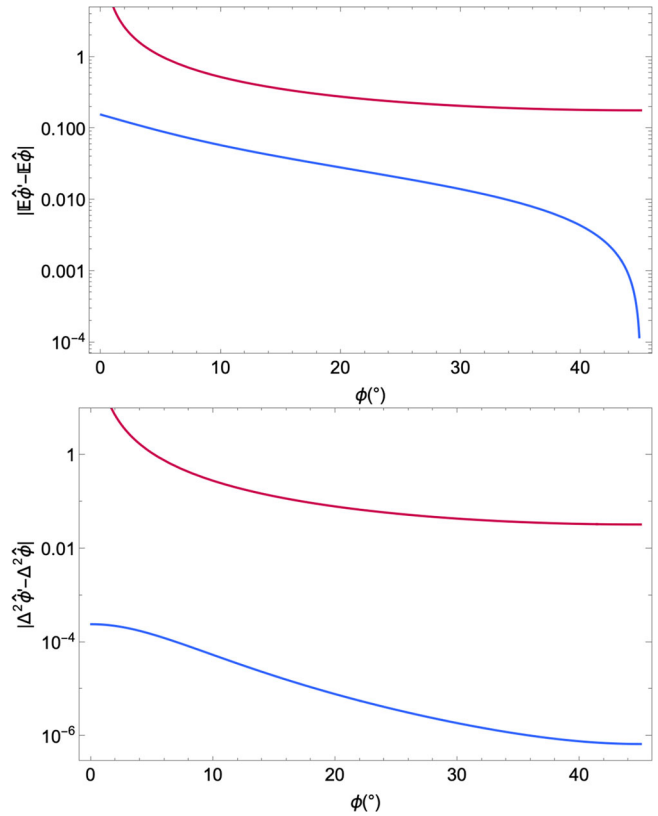


Fig. 5 | Theoretical results for a dephasing channel $|\psi\rangle\langle\psi| \to p|\psi\rangle\langle\psi| + (1-p)I \otimes Z|\psi\rangle\langle\psi|I \otimes Z$, with $p = 0.9$, *i.e.* for a fidelity 0.95 to the ideal state, based on $N = 1000$ estimation events. Top: bias with respect to the ideal case (blue curve) compared with the bound (6) (red curve). Bottom, discrepancy of the variance with respect to the ideal case (blue curve), compared with the bound (7) (red curve).

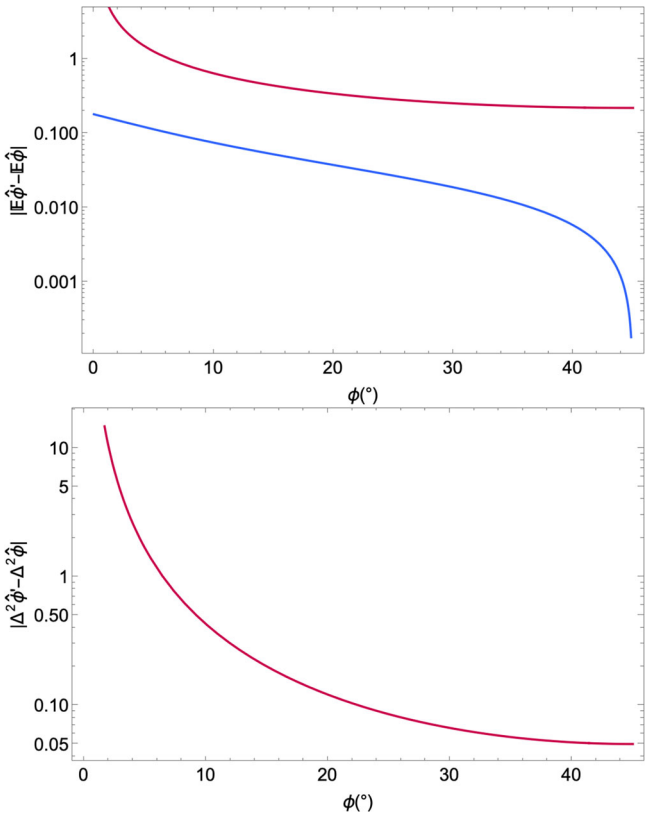


Fig. 6 | Theoretical results for a depolarising channel $|\psi\rangle\langle\psi| \to p|\psi\rangle\langle\psi| + (1-p)I \otimes I/4$, with $p = 0.93$, i.e., for a fidelity 0.95 to the ideal state, based on $N = 1000$ estimation events. Top: bias with respect to the ideal case (blue curve) compared with the bound (6). Bottom, the bounds (7) for the variance discrepancy. Its theoretical value is identically 0, not visible in the logarithmic scale.

$$\langle Y \otimes \mathbf{Y}\rangle = \frac{\mathrm{Tr}[\mathbf{Y}\cdot\Phi(|\mathbf{R}\rangle\langle\mathbf{R}|)] - \mathrm{Tr}[\mathbf{Y}\cdot\Phi(|\mathbf{L}\rangle\langle\mathbf{L}|)]}{2}, \tag{11}$$

where we have used that

$$|\psi_+\rangle \equiv \frac{|+\rangle|\mathbf{0}\rangle + |-\rangle|\mathbf{1}\rangle}{\sqrt{2}} \equiv \frac{|R\rangle|\mathbf{R}\rangle + \mathrm{i}|L\rangle|\mathbf{L}\rangle}{\sqrt{2}} \tag{12}$$

and the fact that the channel controlled by Eve acts only on the B-register, leaving the A-register invariant. We identify in the above expressions differences of expectations of Pauli-like operators on their evolved $+$ 1-eigenstates under Φ. Furthermore, we notice that, for any **P,**

$$\langle\mathbf{P}\rangle = \mathrm{Tr}[\mathbf{P}\cdot\Phi(|\mathbf{P},+\rangle\langle\mathbf{P},+|)] = 2F(|\mathbf{P},+\rangle, \Phi(|\mathbf{P},+\rangle\langle\mathbf{P},+|)) - 1 \equiv 2\widehat{F}_{\mathbf{P}} - 1. \tag{13}$$

Plugging these into (4), we obtain

$$\widehat{F} = \tfrac{1}{4}\left(1 + \tfrac{1}{2}\sum_{\mathbf{P}}(2\widehat{F}_{\mathbf{P}} - 1)\right). \tag{14}$$

Therefore, if $\widehat{F}_{\mathbf{P}} \geq 1 - \bar{\epsilon}^2$ for all **P** in Protocol 2, then in Protocol 1 it holds $\widehat{F} \geq 1 - \epsilon^2$, with $\epsilon^2 = 3\bar{\epsilon}^2/2$. Furthermore, using (9), (10) it is straightforward to show that the estimation step calculates the very same quantity in both protocols. Finally, the expected number of rounds in Protocol 2 is the same.

Finally, observe that both protocols can be carried out in a permutation-invariant way with respect to the different rounds, thanks to the randomization of measurements and actions that Alice and Bob undertake; this is crucial for a reduction of GC attacks to individual ones.

Protocol 2. **One-way MUB-based DQS**

1. *Preparation*: Alice prepares the n-qubit probe state $|\mathbf{P},+\rangle$ for $\mathbf{P} \in \{\pm\mathbf{X}, \pm\mathbf{Y}, \pm\mathbf{Z}\}$ chosen uniformly at random and sends it to Bob via the quantum channel.
2.
3. *Encoding*: Bob chooses to perform one of these three actions at random:

(a) with probability p_c he does not encode the phase;
(b) with probability p_e, he encodes the phase by applying $U(\phi)$ to the received state;
(c) with probability $p_d = 1 - p_c - p_e$, he discards the received state and moves on to the next round of the protocol.

4. *Measurement*: Bob performs one of these two actions, depending on what he did at step 3:

(a) if he did not encode the phase, he measures one of the observables **X**, **Y**, **Z**, chosen uniformly at random;
(b) if he encoded the phase, then he measures one of the observables **X**, **Z**, chosen uniformly at random;

5. *Reconciliation and sifting*: After T repetitions of steps 1-4, Alice communicates to Bob the probe state $|\mathbf{P},+\rangle$ that she employed at each round. Bob then keeps all rounds in which he measured $\pm\mathbf{P}$, discarding the others.
6. *Fidelity check*: From the rounds (a) where he did not encode the phase, Bob estimates the fidelity of the received state with the ideal state $|\mathbf{P},+\rangle$ as $\widehat{F}_{\mathbf{P}} = (\langle\mathbf{P}\rangle + 1)/2$, where the expectation is taken

with respect to the tampered state. If $\widehat{F}_{\mathbf{P}} \geq 1 - \bar{\epsilon}^2$ for all $\mathbf{P}$ and a given safety threshold $\bar{\epsilon}$, then Bob proceeds to the next step 7. Otherwise, he aborts the protocol.

7. *Phase estimation*: From the rounds (b) where he applied $U(\phi)$, Bob estimates the phase as

$$\frac{1}{2}\arccos\left(\frac{1}{4}\sum_{\mathbf{P}\in\{\pm\mathbf{X},\pm\mathbf{Z}\}}\langle\mathbf{P}\rangle\right), \tag{15}$$

where the expectation is taken with respect to the phase-encoded tampered state.

The protocol's faithfulness under GC attacks relies on a de Finetti theorem for adaptive measurements. The basic idea is that, if we look at a small part of a large entangled system, this is approximately separable. At variance with the standard[35] for QKD, here we employ a more refined version of the theorem, due to[27] (see also[36]), which applies to states processed using LOCC_1 measurements, i.e., local measurements performed in a sequential adaptive fashion; these are defined, along with a suitable distance measure, as follows:

Definition 3. (LOCC_1 channel and distance) Let Λ be a quantum channel (CPTP map) acting on $\mathcal{D}(\mathcal{H}^{\otimes n})$. Then Λ is LOCC_1 if it can be written as

$$\Lambda = \Lambda_1 \otimes \cdots \otimes \Lambda_n, \tag{16}$$

where Λ_j for all $j = 1, \cdots, n$, are measurement channels, i.e.,

$$\Lambda_j(\rho) = \sum_i |i\rangle\langle i|\mathrm{Tr}[L_i^{(j)}\rho] \tag{17}$$

for $\{L_i^{(j)}\}_i$ a POVM and $\{|i\rangle\}_i$ a set of orthonormal states, such that $\Lambda_j = \Lambda_{j|1,\cdots,j-1}$ can depend on the measurement outcomes on the previous $j-1$ parties.

Given two quantum states $\rho, \sigma \in \mathcal{D}(\mathcal{H}^{\otimes n})$, their LOCC_1-distance is

$$D_{\mathrm{LOCC}_1}(\rho,\sigma) = \max_{\Lambda\,\mathrm{LOCC}_1} D(\Lambda(\rho),\Lambda(\sigma)). \tag{18}$$

Note that we employ a de Finetti theorem for the LOCC_1-distance, rather than the standard trace-distance, because it provides a more favourable scaling in terms of the number of discarded rounds, while at the same time it does not compromise the estimation performance. Indeed, the deviation of bias and variance on the true probe state with respect to those on the ideal state can be bounded (see Lemma 3) by product observables and hence using the LOCC_1-distance, rather than the trace-distance, which in general is larger.

Clearly, D_{LOCC_1} satisfies the standard properties of a distance. Moreover, $D_{\mathrm{LOCC}_1} \leq D$ and a suitable gentle-measurement lemma[37] for D_{LOCC_1} holds:

Lemma 2. (Gentle measurement for LOCC_1-distance)Let $\mathbb{1} \geq E \geq 0$ be a measurement operator and τ, σ two quantum states. Then

$$\mathrm{Tr}[E\sigma] \geq \mathrm{Tr}[E\tau] - 2D_{\mathrm{LOCC}_1}(\tau,\sigma). \tag{19}$$

Proof. Using (18) and the variational formulation of trace-distance, we have

$$2D_{\mathrm{LOCC}_1}(\tau,\sigma) = \max_{\substack{\Lambda\,\mathrm{LOCC}_1,\\ \mathbb{1}\geq E\geq 0}} \mathrm{Tr}[\mathrm{E}\cdot\Lambda(\tau-\sigma)] \geq \mathrm{Tr}[\mathrm{E}\tau] - \mathrm{Tr}[\mathrm{E}\sigma], \tag{20}$$

where the inequality follows by choosing a specific E and $\Lambda = \mathrm{Id}$. The result follows by rearranging terms, and one can easily switch the roles of τ and σ.

Furthermore, note that our Protocol 2 is clearly contained in the LOCC_1 measurement subset, which guarantees a better scaling of the error term.

We will make use of the following de Finetti theorem for the LOCC_1-distance:

Theorem 2. (Quantum de Finetti for LOCC_1-distance [27, Theorem 1]) Let $\sigma \in \mathcal{D}(\mathcal{H}^{\otimes n})$ be a permutation-invariant state, and $d = \dim(\mathcal{H})$. Then for any integer $1 \leq k \leq m$ there exists a measure μ on $\mathcal{D}(\mathcal{H})$ such that

$$D_{\mathrm{LOCC}_1}\left(\mathrm{Tr}_{m-k}[\sigma], \int d\mu(\rho)\rho^{\otimes k}\right) \leq (k-1)\sqrt{\frac{\log d}{2(m-k)}}. \tag{21}$$

Using these instruments, we prove that Bob or Alice can bound the fidelity to the ideal state on the N_e estimation rounds via the same quantity on the N_c check rounds. This, in turn, implies a bound on the LOCC_1-distance that quantifies Eve's tampering.

Theorem 3. (Tampering quantification for MUB-based protocol under GC attacks) In Protocol 2, let $N_c \geq N_e$, $V(\phi) = U(\phi)^{\otimes N_e}$, and consider a random probe-state $|\mathbf{P},+\rangle$ prepared by Alice, for any $\mathbf{P} \in \{\pm\mathbf{X}, \pm\mathbf{Y}, \pm\mathbf{Z}\}$. Then the LOCC_1-distance between the ideal and tampered state after phase-encoding can be bounded in terms of the fidelity $\widehat{F}_{\mathbf{P}}$ as follows:

$$\begin{aligned} &D_{\mathrm{LOCC}_1}(V(\phi)|\mathbf{P},+\rangle^{\otimes N_e}, V(\phi)\mathrm{Tr}_{T-N_e}[\widetilde{\sigma}]V(\phi)^\dagger) \\ &\leq \sqrt{1-\widehat{F}_{\mathbf{P}} + 4f(T,N_d,n)}. \end{aligned} \tag{22}$$

where $\widetilde{\sigma} = \Phi((|\mathbf{P},+\rangle\langle\mathbf{P},+|)^{\otimes T})$ is the collective tampered state after T rounds of the protocol, with Φ the Eve-controlled collective quantum channel.

Proof. Define $|\psi\rangle = |\mathbf{P},+\rangle$. We want to bound the LOCC_1-distance between the ideal and tampered state during estimation rounds:

$$D_{\mathrm{LOCC}_1}(V(\phi)|\psi\rangle^{\otimes N_e}, V(\phi)\mathrm{Tr}_{T-N_e}[\widetilde{\sigma}]V(\phi)^\dagger) \tag{23}$$

$$= D_{\mathrm{LOCC}_1}(|\psi\rangle^{\otimes N_e}, \mathrm{Tr}_{T-N_e}[\widetilde{\sigma}]) \tag{24}$$

$$\leq \sqrt{1-F(|\psi\rangle^{\otimes N_e}, \mathrm{Tr}_{T-N_e}[\widetilde{\sigma}])}. \tag{25}$$

Since Bob's actions over T rounds are permutation-invariant, the state $\widetilde{\sigma}$ can be taken permutation-invariant too without loss of generality, hence Theorem 2 (with $m = T$, $k = T - N_d$ and $d = 2^n$) implies the existence of a measure $d\mu(\rho)$ on states $\rho \in \mathcal{D}(\mathcal{H})$ such that

$$D_{\mathrm{LOCC}_1}\left(\widetilde{\sigma}, \int d\mu(\rho)\rho^{\otimes T}\right) \leq f(T,N_d,n) := (T-N_d-1)\sqrt{\frac{n}{2N_d}}. \tag{26}$$

We then apply Lemma 2 twice: firstly, for the check rounds with $\tau = \mathrm{Tr}_{T-N_c}[\widetilde{\sigma}]$, $\sigma = \int d\mu(\rho)\rho^{\otimes N_c}$ and $E = (|\psi\rangle\langle\psi|)^{\otimes N_c}$, obtaining

$$\int d\mu(\rho)F(|\psi\rangle,\rho)^{N_c} \geq F(|\psi\rangle^{\otimes N_c}, \mathrm{Tr}_{T-N_c}[\widetilde{\sigma}]) - 2f(T,N_d,n), \tag{27}$$

where in the second term we have used (26) and the non-increasing property of trace distance under the map Tr_{T-N_c}; secondly, for the estimation rounds with $\tau = \int d\mu(\rho)\rho^{\otimes N_e}$, $\sigma = \mathrm{Tr}_{T-N_e}[\widetilde{\sigma}]$ and $E = (|\psi\rangle\langle\psi|)^{\otimes N_e}$, obtaining

$$F(|\psi\rangle^{\otimes N_e}, \mathrm{Tr}_{T-N_e}[\widetilde{\sigma}]) \geq \int d\mu(\rho)F(|\psi\rangle,\rho)^{N_e} - 2f(T,N_d,n). \tag{28}$$

Finally, putting ((27),(28)) together and using the fact that $x^{N_e} \geq x^{N_c}$ for $1 \geq x \geq 0$ and $N_c \geq N_e$ we obtain

$$F(|\psi\rangle^{\otimes N_e}, \mathrm{Tr}_{T-N_e}[\bar{\sigma}]) \geq F(|\psi\rangle^{\otimes N_c}, \mathrm{Tr}_{T-N_c}[\bar{\sigma}]) - 4f(T, N_d, n). \quad (29)$$

In the above expression, the first term on the right-hand side can be estimated by $\widehat{F}_{\mathbf{p}}$. Hence, plugging the expression into (51), we obtain (22).

The bound ensures that the estimate of Eve's tampering during check rounds is also a good estimate for the estimation rounds, even in the case of GC attacks that can introduce correlations between different rounds. This can be guaranteed by making f sufficiently small, i.e., discarding $N_d \gg N_c \geq N_e$ rounds.

The last step is to employ Theorem 3 to quantify how much the phase-estimation results using a tampered state differ from the ideal case, as measured by bias and variance to the true phase. In order to do this, we first have to show that the LOCC_1-distance can be used to bound the deviation of local observables on collective states.

Lemma 3. (Uniform continuity of expectation with respect to LOCC_1-distance) Let A be a local observable on $\mathcal{D}(\mathcal{H}^{\otimes m})$, given by the sum of at most K product observables bounded by a, i.e., $A = \sum_{k=1}^{K} A_{1,k} \otimes \cdots \otimes A_{m,k}$ with $A_{j,k}$ observables on $\mathcal{D}(\mathcal{H})$ for all $j = 1, \cdots, m$ and $k = 1, \cdots, K$, and $||A_{1,k} \otimes \cdots \otimes A_{m,k}||_\infty \leq a$. Then for any two states $\sigma, \sigma' \in \mathcal{D}(\mathcal{H}^{\otimes m})$ it holds

$$\left|\mathrm{Tr}[\mathrm{A}(\sigma - \sigma')]\right| \leq 2aK \cdot D_{\mathrm{LOCC}_1}(\sigma, \sigma'). \quad (30)$$

Proof. Let $A_{j,k} = \sum_{i=1}^{d} a_{i,j,k} \left|a_{i,j,k}\right\rangle\left\langle a_{i,j,k}\right|$ be the spectral decomposition of the local observables constituting A, and define the measurement channels $\Omega_{j,k}(\rho) = \sum_{i=1}^{d} |i\rangle\langle i| \left\langle a_{i,j,k}\middle|\rho\middle|a_{i,j,k}\right\rangle$ for all $\rho \in \mathcal{D}(\mathcal{H})$, $j = 1, \cdots, m$ and $k = 1, \cdots, K$. Then for any $\sigma, \sigma' \in \mathcal{D}(\mathcal{H}^{\otimes n})$ it holds

$$\left|\mathrm{Tr}[\mathrm{A}(\sigma - \sigma')]\right| \leq \sum_{k=1}^{K} \left|\mathrm{Tr}[(\mathrm{A}_{1,\mathrm{k}} \otimes \cdots \otimes \mathrm{A}_{\mathrm{m,k}})(\sigma - \sigma')]\right| \quad (31)$$

$$\leq a \sum_{k=1}^{K} ||(\Omega_{1,k} \otimes \cdots \otimes \Omega_{m,k})(\sigma - \sigma')||_1 \quad (32)$$

$$\leq 2aK \max_{\Omega \mathrm{LOCC}_1} D(\Omega(\sigma), \Omega(\sigma')) \quad (33)$$

$$= 2aK\, D_{\mathrm{LOCC}_1}(\sigma, \sigma'). \quad (34)$$

□

In particular, if an estimation procedure is based on the measurement of a local observable O, which is the case of our protocols, we can use Lemma 3 to bound the difference in bias and variance of the estimation with respect to an ideal state σ, when the latter is tampered into σ'. This generalizes [6, Theorem 1] to the case of non-iid samples which are close in LOCC_1-distance. Importantly, at variance with the previous work, here the bound on the variance has a dependence on ϵ rather than ϵ/m. This is due to our relaxation of the iid assumption for the states σ, σ', which is necessary to contemplate GC attacks.

Theorem 4. (Estimation performance under LOCC_1-tampering) Let O be an o-bounded observable on $\mathcal{H}$, and $\sigma, \sigma' \in \mathcal{D}(\mathcal{H}^{\otimes m})$ two quantum states such that $D_{\mathrm{LOCC}_1}(\sigma, \sigma') \leq \epsilon$. Define $\bar{O} = \frac{1}{m}\sum_{j=1}^{m} O_j \otimes \mathbb{1}^{\otimes(m-1)}$ as the m-partite average of O, $\mathbb{E}_\sigma \bar{O} = \mathrm{Tr}[\bar{O}\sigma]$ as its expectation on σ, and $\Delta^2_{\sigma_0,\sigma} \bar{O} = \mathrm{Tr}[(\bar{O} - \mathbb{E}_{\sigma_0}\bar{O})^2\sigma]$ as the variance of its estimation on σ with respect to the state σ_0.

Then, the difference in the expectation of $\bar{O}$ on the two states is bounded as

$$\left|\mathbb{E}_\sigma \bar{O} - \mathbb{E}_{\sigma'} \bar{O}\right| \leq 2o\epsilon, \quad (35)$$

while the difference in the variance of the estimation of $\bar{O}$ with respect to the state σ is bounded as

$$\left|\Delta^2_{\sigma,\sigma} \bar{O} - \Delta^2_{\sigma,\sigma'} \bar{O}\right| \leq 4o^2(2\epsilon + \epsilon^2). \quad (36)$$

Proof. To prove the bound for the expectation, we apply Lemma 3 with $A = \bar{O}$. This implies $a = o/m$ and $K = m$, and we obtain

$$\left|\mathbb{E}_\sigma \bar{O} - \mathbb{E}_{\sigma'} \bar{O}\right| = \left|\mathrm{Tr}[\mathrm{A}(\sigma - \sigma')]\right| \leq 2o\epsilon. \quad (37)$$

To prove the inequality for the variance, following[6], we first note that

$$\Delta^2_{\sigma,\sigma'} \bar{O} = \mathrm{Tr}[(\bar{O} - \mathbb{E}_{\sigma'}\bar{O} + \mathbb{E}_{\sigma'}\bar{O} - \mathbb{E}_\sigma \bar{O})^2 \sigma'] \quad (38)$$

$$= \mathrm{Var}_{\sigma'} \bar{O} + \left(\mathbb{E}_{\sigma'}\bar{O} - \mathbb{E}_\sigma \bar{O}\right)^2 \quad (39)$$

with $\mathrm{Var}_\sigma \bar{O} = \Delta^2_{\sigma,\sigma} \bar{O}$, and hence

$$\left|\Delta^2_{\sigma,\sigma} \bar{O} - \Delta^2_{\sigma,\sigma'} \bar{O}\right| \leq \left|\mathrm{Var}_\sigma \bar{O} - \mathrm{Var}_{\sigma'} \bar{O}\right| + \left(\mathbb{E}_{\sigma'}\bar{O} - \mathbb{E}_\sigma \bar{O}\right)^2. \quad (40)$$

The second term above can be bounded by $(2o\epsilon)^2$ via (35). For the first one, instead, we can write

$$\mathrm{Var}_\sigma \bar{O} = \mathrm{Tr}[O^2\sigma] - (\mathrm{Tr}[O\sigma])^2 = \mathrm{Tr}[(O^2 \otimes \mathbb{1} - O^{\otimes 2})\sigma^{\otimes 2}]. \quad (41)$$

Therefore, we can apply Lemma 3 with $A = \frac{1}{m}\sum_{j=1}^{m}(O^2 \otimes \mathbb{1} - O^{\otimes 2})_j \otimes \mathbb{1}^{\otimes(m-1)}$ on two copies of the states, satisfying $D_{\mathrm{LOCC}_1}(\sigma^{\otimes 2}, \sigma'^{\otimes 2}) \leq 2\epsilon$. This implies $a = 2o^2/m$ and $K = m$, and we obtain

$$\left|\Delta^2_{\sigma,\sigma} \bar{O} - \Delta^2_{\sigma,\sigma'} \bar{O}\right| \leq \mathrm{Tr}\left[\mathrm{A}(\sigma^{\otimes 2} - \sigma'^{\otimes 2})\right] + 4o^2\epsilon^2 \quad (42)$$

$$\leq 4o^2 \cdot 2\epsilon + 4o^2\epsilon^2 = 4o^2(2\epsilon + \epsilon^2). \quad (43)$$

□

We are now ready to prove the security and faithfulness of the MUB-based protocol:

Theorem 5. The one-way MUB-based DQS Protocol 2 is perfectly secure and its faithfulness is determined by ϵ. Indeed, the difference of bias and variance of the unbiased estimator $\widehat{\phi}$ calculated on the ideal probe state with respect to the same estimator $\widehat{\phi}'$ on the tampered state are bounded, under GC attacks, as

$$\left|\mathbb{E}\widehat{\phi} - \mathbb{E}\widehat{\phi}'\right| \leq \frac{\epsilon_0}{n|\sin(2n\phi)|}, \quad (44)$$

$$\left|\Delta^2\widehat{\phi} - \Delta^2\widehat{\phi}'\right| \leq \frac{(2\epsilon_0 + \epsilon_0^2)}{n^2\sin^2(2n\phi)}. \quad (45)$$

with $\epsilon_0 = \sqrt{\bar{\epsilon}^2 + 4f(T, N_d, n)}$. In the case of individual attacks, one can take $N_d = 0$ and employ the same bias bound of (6) with $\epsilon_0 \mapsto \bar{\epsilon}$, while the variance bound reads

$$\left|\Delta^2\widehat{\phi} - \Delta^2\widehat{\phi}'\right| \leq \frac{(2\bar{\epsilon}/N_e + \bar{\epsilon}^2)}{n^2\sin^2(2n\phi)}. \quad (46)$$

The two-way version of the protocol has similar bounds with $\epsilon_0 \mapsto \sqrt{\bar{\epsilon}^2 + 2f(T, N_d, n)} + |\sin(\min\{n\phi, \pi/2\})|$, where $\delta(U)$ is the minimum arc-length on the unit-circle that contains all eigenvalues of U.

Proof. Perfect security in the one-way protocol is straightforward to prove. Indeed, even though Eve can fully control the quantum state received by Bob, e.g., by replacing it with a known probe state, she cannot measure said state nor access Bob's measurement outcomes to estimate the phase.

As for faithfulness, if the check step passes, the protocol guarantees that $\widehat{F}_{\mathbf{P}} \geq 1 - \bar{\epsilon}^2$ for all $\mathbf{P}$. Hence, by Theorem 3, the estimation rounds are ϵ_0-close to ideal for all $\mathbf{P}$, i.e.,

$$D_{\mathrm{LOCC}_1}(V(\phi)|\mathbf{P}, +\rangle^{\otimes N_e}, V(\phi)\mathrm{Tr}_{T-N_e}[\widetilde{\sigma}]V(\phi)^\dagger) \leq \epsilon_0. \tag{47}$$

Combining this estimate with Theorem 4, with $O = \mathbf{P} \in \{\pm\mathbf{X}, \pm\mathbf{Z}\}$ and $o = 1$ we obtain

$$\left|\mathbb{E}_\sigma \bar{O} - \mathbb{E}_{\sigma'} \bar{O}\right| \leq 2\epsilon_0, \tag{48}$$

$$\left|\Delta^2_{\sigma,\sigma} \bar{O} - \Delta^2_{\sigma,\sigma'} \bar{O}\right| \leq 4(2\epsilon_0 + \epsilon_0^2). \tag{49}$$

The bias and variance on the estimator are obtained via error propagation, rescaling by

$$|\partial_\theta \langle O\rangle| = |\partial_\theta \cos(n\phi)| = n|\sin(n\phi)|, \tag{50}$$

or its square, where the expectation is taken with respect to the phase-encoded ideal state $e^{-i\frac{\phi}{2}\mathbf{Y}}|\mathbf{P}, +\rangle$ for each $\mathbf{P}$.

If we restrict to individual attacks, Theorem 3 simplifies considerably since the collective state $\widetilde{\sigma} = \widetilde{\rho}^{\otimes T}$ is a product state with respect to each round, so that we can apply directly the bias and variance bounds of ref. 6. Then, calling $W(\phi) = e^{-i\frac{\phi}{2}Y}$, we have

$$D(W(\phi)|\mathbf{P}, +\rangle, W(\phi)\widetilde{\rho}W(\phi)^\dagger) \tag{51}$$

$$\leq \sqrt{1 - F(|\mathbf{P}, +\rangle, \widetilde{\rho})} \leq \bar{\epsilon}, \tag{52}$$

where we have used the unitary-invariance of the trace-distance and the Fuchs-Van-der-Graf inequality, and the fidelity to the ideal state is estimated as $\widehat{F}_{\mathbf{P}}$ from the check rounds.

The proof of Theorem 1 follows straightforwardly by combining Theorem 5 with Lemma 1 above.

Faithfulness proof for the two-way protocol

Here we consider the extension of our one-way protocols to a two-way scenario. As already noted, the form of both Protocols 1 and 2 has very minor changes, essentially with Bob sending Alice the quantum state after the Encoding step and Alice replacing Bob's role in all following steps.

As also noted above, the security of the protocol cannot be guaranteed in this case. Indeed, while one could imagine to have Bob disclose the estimation rounds only after Alice has checked for the presence of Eve, this latter task is harder than it appears. In particular, it is hard for Alice to quantify, from her received state, how much information might have leaked to Eve.

In the following, we thus focus on faithfulness under GC attacks, which can be guaranteed also in this case.

Proof. (Proof of the two-way part of Theorem 5) With respect to the one-way protocol, in the two-way case the major difficulty is that Eve can interact with the quantum state both before and after Bob, possibly even employing a quantum memory. This makes the estimation of tampering on the estimation rounds from the check rounds more difficult, changing Theorem 3. We refer to the communication rounds from Alice to Bob as *forth* communication and to those from Bob to Alice as *back* communication. After T rounds, and before any measurement takes place, the quantum state held by Alice can be written as

$$\widetilde{\tau}(\phi) = \mathrm{Tr}_E[W(V(\phi) \otimes \mathbb{1})\widetilde{\sigma}_{BE}(V(\phi) \otimes \mathbb{1})W^\dagger], \tag{53}$$

where $\widetilde{\sigma}_{BE}$ is the state shared by Bob and Eve after T transmissions from Alice to Bob and W is a unitary dilation of Eve's back channel acting on the states that Bob sends to Alice. Note that also in this case the state $\widetilde{\sigma}$ can be taken permutation-invariant, as the protocol still employs randomized measurements.

We can then bound the LOCC_1-distance to the ideal phase-encoded state similarly to the one-way case:

$$D_{\mathrm{LOCC}_1}(V(\phi)|\psi\rangle^{\otimes N_e}, \mathrm{Tr}_{T-N_e}[\widetilde{\tau}(\phi)]) \tag{54}$$

$$\leq D_{\mathrm{LOCC}_1}\left(V(\phi)|\psi\rangle^{\otimes N_e}, \int d\mu(\rho)\rho^{\otimes N_e}\right) + f(T, N, n). \tag{55}$$

where the inequality follows from Theorem 2, with the same quantities as defined for (26) and the second argument of the LOCC_1-distance can be ϕ-dependent. The first term above can be treated as follows:

$$D_{\mathrm{LOCC}_1}\left(V(\phi)|\psi\rangle^{\otimes N_e}, \int d\mu(\rho)\rho^{\otimes N_e}\right) \tag{56}$$

$$\leq D_{\mathrm{LOCC}_1}\left(V(\phi)|\psi\rangle^{\otimes N_e}, \int d\mu(\rho)V(\phi)\rho^{\otimes N_e}V(\phi)^\dagger\right) \tag{57}$$

$$+D\left(\int d\mu(\rho)V(\phi)\rho^{\otimes N_e}V(\phi)^\dagger, \int d\mu(\rho)\rho^{\otimes N_e}\right) \tag{58}$$

$$\leq \sqrt{1 - \int d\mu(\rho)F(|\psi\rangle\langle\psi|, \rho)^{N_e}} + \int d\mu(\rho)D(V(\phi)\rho^{\otimes N_e}V(\phi)^\dagger, \rho^{\otimes N_e}) \tag{59}$$

$$\leq \sqrt{1 - F((|\psi\rangle\langle\psi|)^{\otimes N_c}, \mathrm{Tr}_{T-N_c}[\widetilde{\sigma}_B]) + 2f(T, N, n)} + \int d\mu(\rho)D(V(\phi)\rho^{\otimes N_e}V(\phi)^\dagger, \rho^{\otimes N_e}), \tag{60}$$

where, in the first term of the last inequality, we have used (27) and the fact that $x^{N_e} \geq x^{N_c}$ for $1 \geq x \geq 0$ and $N_c \geq N_e$, and $\widetilde{\sigma}_B = \mathrm{Tr}_E[\widetilde{\sigma}_{BE}]$.

For the second term in (60), instead, we need to bound the distance between a product state ρ^{N_c} and its rotated version under $V(\phi)$, proceeding as follows:

$$D(\rho^{N_c}, V(\phi)\rho^{N_c}V(\phi)) \leq \sqrt{1 - F(\rho, U(\phi)\rho U(\phi)^\dagger)^{N_e}} \leq \sqrt{1 - F(|\nu\rangle, (U(\phi) \otimes \mathbb{1})|\nu\rangle)^{N_e}} \tag{61}$$

where in the first equality we have used the Fuchs-van-de-Graf inequality and recalled that $V(\phi) = U(\phi)^{\otimes N_e}$, while in the second one the non-increasing property of trace-distance under the partial-trace channel and $|\nu\rangle$ is a purification of ρ. Finally, taking the worst-case over all possible states $|\nu\rangle$, we obtain

$$D(\rho^{N_c}, V(\phi)\rho^{N_c}V(\phi)) \leq \sqrt{1 - \min_{|\nu\rangle} F(|\nu\rangle, (U(\phi) \otimes \mathbb{1})|\nu\rangle)^{N_e}}, \tag{62}$$

which corresponds to Eve being able to discriminate the presence or absence of $U(\phi)$ with the largest success probability allowed by quantum mechanics.

This problem has been studied by Acin[38], who proved that

$$\min_{|v\rangle} F(|v\rangle, U(\phi)|v\rangle) = \cos^2 \min\left\{\frac{\delta(U(\phi))}{2}, \frac{\pi}{2}\right\}, \tag{63}$$

where δ is the minimum arc-length on the unit-circle that contains all eigenvalues of U. Putting all together we obtain the bound

$$D_{\mathrm{LOCC}_1}\left(V(\phi)|\psi\rangle^{\otimes N_\epsilon}, \int d\mu(\rho)\rho^{\otimes N_\epsilon}\right) \leq \sqrt{1 - F((|\psi\rangle\langle\psi|)^{\otimes N_\epsilon}, \mathrm{Tr}_{T-N_\epsilon}[\widetilde{\sigma}_B]) + 2f(T,N,n)} \tag{64}$$

$$+\left|\sin\frac{\min\{\delta(U(\phi)), \pi\}}{2}\right| \tag{65}$$

Note that, in our case,

$$U(\phi) = (e^{-i\phi}|R\rangle\langle R| + e^{i\phi}|L\rangle\langle L|)^{\otimes n} \tag{66}$$

has eigenvalues $\lambda_j = e^{-in\phi(1-2j)}$ for $j = 0, \cdots, n$. Hence $\delta(U(\phi)) = 2n\phi$ for $n\phi < \pi$. Finally, the distance bound (64) can be employed as in the one-way case to obtain the theorem statement. □

Experimental methods

The photon source is a 3-mm beta-barium borate crystal pumped by a CW laser at 405 nm—see Fig. 2. The downconversion emission is collected by single-mode fibres through interference filters with 7.5 nm full width at half maximum. Photons are then delivered to a partially polarising beam splitter (PPBS) $T_H = 1$, $T_V = 1/3$), both with the polarisation $|\widetilde{D}\rangle = (|H\rangle + \sqrt{3}|V\rangle)/2$ (H is the horizontal polarisation, V the vertical, D diagonal at 45°, A diagonal at 135°, L left-circular, R right-circular). This is chosen in such a way to produce a maximally entangled state $|\psi\rangle = (|HD\rangle + VA)/\sqrt{2}$ by nonclassical interference, postselecting on coincidence events[39–41]. The system is embedded in a Sagnac interferometer in order to curtail the impact of imperfect transimittivities of the PPBS (not shown in the figure)[42–44].

Polarisation is then analysed by means of a standard arrangement of a half-wave plate (HWP), a quarter-wave plate (QWP), and a PBS. Acquisition windows are set as 0.1 ns, each containing around 100 coincidence detection events. Each correlator, used to either the check or the estimation rounds, is reconstructed as

$$\langle A \otimes B\rangle = \frac{\sum_{i,j}(-1)^{i+j}N_{ij}}{\sum_{i,j}N_{ij}} \quad i,j = 0,1 \tag{67}$$

where A and B are the proper Pauli operators X, Y or Z, and $N_{i,j}$ are the coincidence counts registered—$i = 0$ corresponds to D, L or $H, i = 1$ to A, R or V, respectively for the three observables. Fidelity is estimated from events collected in 200 detection windows. The phases in Fig. 3 are the average over 200 values, each one derived from a distinct detection window. The uncertainty on the phase is obtained by error propagation on (67), leading to

$$\Delta^2\widehat{\phi}' = \frac{\Delta^2(Z\otimes X) + \Delta^2(X\otimes Z)}{4\left(4 - \left(\langle X\otimes Z\rangle + \langle Z\otimes X\rangle\right)^2\right)}. \tag{68}$$

Here the bar stands for the average over the 200 experimental values.

Data availability

The data supporting our findings are available on a public-access repository at https://doi.org/10.5281/zenodo.15271379.

Received: 21 May 2025; Accepted: 31 December 2025;
Published online: 17 January 2026

References

1. Giovannetti, V., Lloyd, S. & Maccone, L. Advances in quantum metrology. *Nat. Photonics* **5**, 222–229 (2011).
2. Yin, P. et al. Experimental demonstration of secure quantum remote sensing. *Phys. Rev. Appl.* **14**, 014065 (2020).
3. Takeuchi, Y., Matsuzaki, Y., Miyanishi, K., Sugiyama, T. & Munro, W. J. Quantum remote sensing with asymmetric information gain. *Phys. Rev. A* **99**, 022325 (2019).
4. Moore, S. W. & Dunningham, J. A. Secure quantum remote sensing without entanglement. *AVS Quantum Sci.* **5**, 014406 (2023).
5. Huang, Z., Macchiavello, C. & Maccone, L. Cryptographic quantum metrology. *Phys. Rev. A* **99**, 022314 (2019).
6. Shettell, N., Kashefi, E. & Markham, D. Cryptographic approach to quantum metrology. *Phys. Rev. A* **105**, L010401 (2022).
7. Rogers, A. Distributed optical-fibre sensing. *Meas. Sci. Technol.* **10**, R75 (1999).
8. Qi, H., Iyengar, S. & Chakrabarty, K. Distributed sensor networks-a review of recent research. *J. Frankl. Inst.* **338**, 655–668 (2001).
9. He, Z. & Liu, Q. Optical fiber distributed acoustic sensors: a review. *J. Light. Technol.* **39**, 3671–3686 (2021).
10. Ukil, A., Braendle, H. & Krippner, P. Distributed temperature sensing: review of technology and applications. *IEEE Sensors J.* **12**, 885–892 (2012).
11. Proctor, T. J., Knott, P. A. & Dunningham, J. A. Multiparameter estimation in networked quantum sensors. *Phys. Rev. Lett.* **120**, 080501 (2018).
12. Ge, W., Jacobs, K., Eldredge, Z., Gorshkov, A. V. & Foss-Feig, M. Distributed quantum metrology with linear networks and separable inputs. *Phys. Rev. Lett.* **121**, 043604 (2018).
13. Zhuang, Q., Zhang, Z. & Shapiro, J. H. Distributed quantum sensing using continuous-variable multipartite entanglement. *Phys. Rev. A* **97**, 032329 (2018).
14. Kasai, H., Takeuchi, Y., Hakoshima, H., Matsuzaki, Y. & Tokura, Y. Anonymous quantum sensing. *J. Phys. Soc. Jpn* **91**, 074005 (2022).
15. Guo, X. et al. Distributed quantum sensing in a continuous-variable entangled network. *Nat. Phys.* **16**, 281–284 (2020).
16. Zhao, S.-R. et al. Field demonstration of distributed quantum sensing without post-selection. *Phys. Rev. X* **11**, 031009 (2021).
17. Kómár, P. et al. A quantum network of clocks. *Nat. Phys.* **10**, 582–587 (2014).
18. He, W. et al. Experimental secure entanglement-free quantum remote sensing over 50 km of optical fiber. *Phys. Rev. A.* **111**, 062607 (2025).
19. Xie, D., Xu, C., Chen, J. & Wang, A. M. High-dimensional cryptographic quantum parameter estimation. *Quantum Inf. Process.* **17**, 116 (2018).
20. Ho, J. et al. Quantum-private distributed sensing. Preprint at https://doi.org/10.48550/arXiv.2410.00970 (2024).
21. Hassani, M., Scheiner, S., Paris, M. G. & Markham, D. Privacy in networks of quantum sensors. *Phys. Rev. Lett.* **134**, 030802 (2025).
22. Shettell, N., Hassani, M. & Markham, D. Private network parameter estimation with quantum sensors. Preprint at https://doi.org/10.48550/arXiv.2207.14450 (2022).
23. Liu, Y.-C. et al. Quantum integrated sensing and communication via entanglement. *Phys. Rev. Appl.* **22**, 034051 (2024).
24. Bugalho, L., Hassani, M., Omar, Y. & Markham, D. Private and robust states for distributed quantum sensing. *Quantum* **9**, 1596 (2025).
25. Zang, A. et al. Quantum advantage in distributed sensing with noisy quantum networks. Preprint at https://doi.org/10.48550/arXiv.2409.17089 (2024).
26. Kim, D.-H. et al. Distributed quantum sensing of multiple phases with fewer photons. *Nat. Commun.* **15**, 266 (2024).
27. Li, K. & Smith, G. Quantum de Finetti theorem under fully-one-way adaptive measurements. *Phys. Rev. Lett.* **114**, 160503 (2015).
28. Pirandola, S. et al. Advances in quantum cryptography. *Adv. Opt. Photonics* **12**, 1012 (2020).

29. Shettell, N. & Markham, D. Quantum metrology with delegated tasks. *Phys. Rev. A* **106**, 052427 (2022).
30. Bilkis, M., Rosati, M. & Calsamiglia, J. Reinforcement-learning calibration of coherent-state receivers on variable-loss optical channels. In *Proc. IEEE Information Theory Workshop* 1–6 (IEEE, 2021).
31. Rosati, M. Performance of coherent frequency-shift keying for classical communication on quantum channels. In *Proc. IEEE International Symposium on Information Theory* 902–905 (IEEE, 2021).
32. Rosati, M. & Solana, A. Joint-detection learning for optical communication at the quantum limit. *Opt. Quantum* **2**, 390 (2024).
33. Nötzel, J. & Rosati, M. Operating fiber networks in the quantum limit. *J. Light. Technol.* **41**, 6865–6874 (2023).
34. Munar-Vallespir, P. & Nötzel, J. Joint communication and sensing over the lossy bosonic quantum channel. In *Proc. 10th World Forum Internet Things* 1–6 (IEEE, 2024).
35. Renner, R. Symmetry of large physical systems implies independence of subsystems. *Nat. Phys.* **3**, 645–649 (2007).
36. Brandao, F. G. & Harrow, A. W. Quantum de Finetti theorems under local measurements with applications. In *Proc. 45th Annual ACM Symposium on Theory of Computing* 861–870 (ACM, 2013).
37. Winter, A. Coding theorem and strong converse for quantum channels. *IEEE Trans. Inf. Theory* **45**, 2481–2485 (1999).
38. Acín, A. Statistical distinguishability between unitary operations. *Phys. Rev. Lett.* **87**, 177901 (2001).
39. Langford, N. K. et al. Demonstration of a simple entangling optical gate and its use in bell-state analysis. *Phys. Rev. Lett.* **95**, 210504 (2005).
40. Kiesel, N., Schmid, C., Weber, U., Ursin, R. & Weinfurter, H. Linear optics controlled-phase gate made simple. *Phys. Rev. Lett.* **95**, 210505 (2005).
41. Okamoto, R., Hofmann, H. F., Takeuchi, S. & Sasaki, K. Demonstration of an optical quantum controlled-not gate without path interference. *Phys. Rev. Lett.* **95**, 210506 (2005).
42. Bizzarri, G. et al. Quantum steering from phase measurements with limited resources. *AVS Quantum Sci.* **6**, 024405 (2024).
43. Bizzarri, G. et al. Quasiprobability distributions with weak measurements. *Quantum Sci. Technol.* **10**, 045008 (2025).
44. Bizzarri, G. et al. Controlling sloppiness in two-phase estimation with a tunable weak measurement. *Opt. Quantum* **3**, 432 (2025).

Acknowledgements

We thank F. De Stefani for valuable discussion, and A. Fabbri for assistance with malfunctioning equipment. This work was supported by the PRIN project PRIN22-RISQUE-2022T25TR3 of the Italian Ministry of University. G.B. is supported by Rome Technopole Innovation Ecosystem (PNRR grant M4-C2-Inv). IG acknowledges the support from MUR Dipartimento di Eccellenza 2023-2027. M.R. acknowledges support from the project PNRR - Finanziato dall'Unione Europea—MISSIONE 4 COMPONENTE 2 INVESTIMENTO 1.2—"Finanziamento di progetti presentati da giovani ricercatori"—Id MSCA 0000011-SQUID - CUP F83C22002390007 (Young Researchers)—Finanziato dall'Unione europea - NextGenerationEU.

Author contributions

M.R. elaborated the theory with inputs from G.B. and M.B. G.B. and M.B. carried out the experiment with the assistance of the other authors. G.B., M.B., and M.R. wrote the manuscript and carried out the study. All authors reviewed the manuscript. M.R. supervised the project.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to Matteo Rosati.

Reprints and permissions information is available at http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

© The Author(s) 2026