Private Remote Phase Estimation over a Lossy Quantum Channel

Farzad Kianvash[1], Marco Barbieri[2,3,4], and Matteo Rosati[1]

[1]Dipartimento di Ingegneria Civile, Informatica e delle Tecnologie Aeronautiche, Università degli Studi Roma Tre, Via della Vasca Navale 79, 00146 Rome, Italy
[2]Dipartimento di Scienze, Università degli Studi Roma Tre, Via della Vasca Navale 84, 00146 Rome, Italy
[3]Istituto Nazionale di Ottica - CNR (CNR-INO), Via Nello Carrara 1, Sesto F.no 50019, Italy
[4]INFN, Sezione di Roma Tre, Via della Vasca Navale 84, 00146 Rome, Italy

Abstract

Private remote quantum sensing (PRQS) aims at estimating a parameter at a distant location by transmitting quantum states on an insecure quantum channel, limiting information leakage and disruption of the estimation itself from an adversary. Previous results highlighted that one can bound the estimation performance in terms of the observed noise. However, if no assumptions are placed on the channel model, such bounds are very loose and severely limit the estimation. We propose and analyse a PRQS using, for the first time to our knowledge, continuous-variable states in the single-user setting. Assuming a typical class of lossy attacks and employing tools from quantum communication, we calculate the true estimation error and privacy of our protocol, both in the asymptotic limit of many channel uses and in the finite-size regime. Our results show that a realistic channel-model assumption, which can be validated with measurement data, allows for a much tighter quantification of the estimation error and privacy for all practical purposes.

Introduction – Quantum sensing and cryptography are among the leading applications of modern quantum technologies. In recent years, with the rise of small quantum networks [1, 2], researchers have studied the potential of combining the unique features and advantages of both technologies into a single application. Enter private remote quantum sensing (PRQS), a technique that allows a quantum provider to estimate physical quantities at a distant location, connected via an insecure quantum communication channel [3, 4, 5, 6, 7, 8, 9, 10, 11, 12], with applications to biometry, remote medicine and, more generally, to the remote handling of sensitive data. In this client-server scenario, Alice owns quantum hardware that can produce probes for estimation, while Bob, the other legitimate user, sits at a distant location where the estimation has to take place. Thus, Alice seeks to carry out the estimation remotely, ensuring that Eve, who controls the quantum communication channel, gathers as little information as possible about the estimated parameter and, at the same time, does not spoil the legitimate estimation procedure.

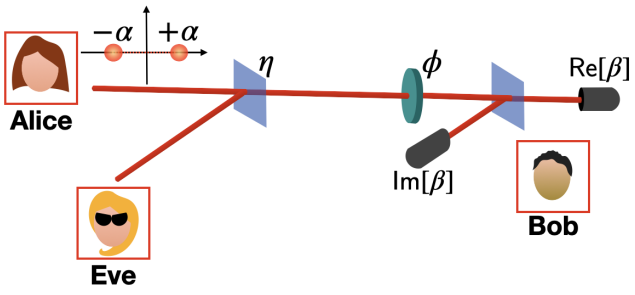

Figure 1: Schematic depiction of our PRQS protocol. Alice wants to estimate a phase ϕ at Bob's location, out of her reach. She thus delegates the measurement to Bob, who performs heterodyne on the transmitted probes. Eve compromises the security of the protocol by tapping part of the signal, in order to learn the initial phase, and can also access any classical communication between the parties.

The PRQS problem has been well-studied using discrete-variable (DV) states in the single-user setting [3, 4, 5, 6, 7, 8, 9, 12], employing tools from quantum cryptography for the analysis of metrologically relevant quantities such as the estimation bias and variance. In the related, but distinct setting of multi-user distributed sensing, research has focused instead on guaranteeing privacy with respect to other users rather than to an eavesdropper [10, 11, 13, 14, 15]. These studies have highlighted the importance of establishing specific figures of merit for the task at hand, in order to put the notions of privacy and integrity on the quantitative level. However, this endeavour has revealed how difficulties may arise in bringing together concepts from cryptography and metrology. In particular, building on previous works in the single-user case, Ref. [12] provided a threshold-based mechanism to check the probe's quality before proceeding to estimation and, with an experimental implementation, uncovered a major shortcoming of current PRQS approaches: while

general limits can be inferred on the sensing performance by analyzing the transmitted probes, these are typically loose, as they have to account for any form of noise added to the probe by Eve. Pursuing an analogy with secure communications, insight in such cases are gained by inspecting specific attack models.

In this work we tackle exactly this issue, proving that the assumption of a specific noise model yields an accurate quantification of Eve's actions. While in theory this effectively restricts Eve's attack class, in practical cryptographic implementations it is common to work with reasonable assumptions on the channel model, which can then be regularly checked using the measurement data gathered for channel parameter estimation. Our work, to the best of our knowledge, pioneers PRQS protocols based on continuous-variable (CV) states in the single-user setting (for the distinct multi-user setting see instead the very recent Refs. [14, 15]). Similarly to the DV case where PRQS schemes are based on seminal QKD protocols such as BB84 and E91 [16, 17], our proposed CV protocol is reminiscent of GG02 [18]. However, in order to provide a realistic protocol and avoid over-simplifications connected with a continuous signal distribution, at variance with GG02 we consider a discrete constellation of probe states [19, 20, 21, 22]. As a consequence, tackling Eve's attacks requires yet again the use of tools from quantum communication: we originally integrate results from minimum-error state discrimination [23, 24, 25, 26, 27, 28] to quantify the attacker's estimation performance under a discrete modulation of the original probe states. Finally, our protocol analysis is valid for any number of channel uses, enabling a complete understanding of security and estimation performance both in the asymptotic limit and in the finite-size regime, which is notoriously hard to tackle in CV-QKD. Therefore, our results are a valuable asset for informing future deployments in real networks.

The protocol – We consider the setting depicted in Fig. 1. At each round of the protocol, Alice transmits a single-mode coherent state of the electromagnetic field, $|\alpha\rangle_i = e^{a^\dagger \alpha_i - a\alpha_i^*}|0\rangle$, over an insecure quantum channel to Bob, where $a, a^\dagger$ are the mode photon-annihilation and -creation operators satisfying the canonical commutation relations $[a, a^\dagger] = 1$. In order to enforce security, Alice picks the coherent-state complex amplitude from a discrete set with fixed mean photon number α^2, i.e., $\alpha_i \in \mathcal{A} = \{\alpha e^{\mathrm{i}\theta_k} : \alpha > 0\}_{k=1}^{A}$. Bob encodes an unknown phase ϕ on the received states via the unitary $R(\phi) = e^{-i\phi a^\dagger a}$ and then performs heterodyne measurements, represented by the positive-operator-valued-measurement $\{\frac{1}{\pi}|\beta\rangle\langle\beta|\}_{\beta\in\mathbb{C}}$, obtaining in the i-th run the outcome β_i. While the scenario in itself is quite general, we assume that Eve can perform only passive attacks: the noise model is a bosonic pure-loss channel, mapping $|\alpha_i\rangle_A \mapsto |\alpha_i\sqrt{\eta}\rangle_B$; therefore, the remaining part of the probe state is intercepted by Eve, i.e., $|\alpha_i\sqrt{1-\eta}\rangle_E$. This restriction has the advantage of providing a clear setting to bound the performance of the PRQS protocol, while retaining a certain level of practical interest. After N rounds, Bob first enters a CHECK phase, employing the measured data to evaluate which fraction of the signal was intercepted by Eve, and determine if that guarantees sufficient privacy upon disclosing the measurement outcomes. If the CHECK is passed, then Bob publicly announces his outcomes $\{\beta_i\}_{i=1}^N$, allowing Alice to proceed with the ESTIMATION phase.

We stress that, since our protocol does not rely directly on the security of GG02, it enables us to privilege considerations on practicality, pointing to the use of a more controlled discrete modulation of Alice's phase [24, 29, 28]. While this compromises the Gaussianity of the overall state, hence requiring greater care in secret key analysis [21, 22], we will show how our PRQS protocol is immune from such limitations, thanks also to the passive-attack assumption.

Binary-phase alphabet – In order to illustrate what happens in each phase specifically, we assume for simplicity the case of a symmetric binary-phase-shift-keyed (BPSK) alphabet $\mathcal{A} = \{\pm\alpha : \alpha \geq 0\}$. In the ESTIMATION phase, Alice corrects Bob's data with her knowledge of the initial phases, obtaining the dataset $\{\beta_i^A = \beta_i \cdot s_i\}_{i=1}^N$, where $s_i = \mathrm{sign}(\alpha_i)$; then, she estimates the phase via the estimator $\hat{\phi}^A = \arg\frac{1}{N}\sum_{i=1}^N \beta_i^A$, which is maximum-likelihood, as shown in the Supplementary Material (SM). Alice's performance is quantified by the mean-square error (MSE). In the local-estimation setting, where the true value of ϕ is approximately known, one studies the local MSE, averaging with respect to the outcome distribution, i.e., $\mathrm{MSE}_A(\phi) = \mathbb{E}_{\{\beta_i^A\}|\phi}(\hat{\phi}^A - \phi)^2$; instead, in the Bayesian setting one studies the average MSE with respect to the phase distribution, i.e., $\mathrm{MSE}_A = \mathbb{E}_\phi \mathrm{MSE}_A(\phi)$. In both cases, the MSE is a function of the received coherent-state amplitude $\sqrt{\eta}\,\alpha$, a priori unknown to the legitimate users due to the loss introduced by Eve. Clearly, in trying to estimate ϕ, Eve will try a similar procedure but will first need to identify the phase of α_i chosen by Alice, via a BPSK discrimination experiment [24]. Eve's error is then quantified by the Helstrom bound [30, 24]: $P_e^{\mathrm{Hel}} = \frac{1}{2}\left(1 - \sqrt{1 - e^{-4(1-\eta)\alpha^2}}\right)$, i.e., with probability $p(\eta) = P_e^{\mathrm{Hel}}$ Eve will identify the wrong phase $\hat{s}_i = -\mathrm{sign}(\alpha_i)$, while with probability $q(\eta) = 1 - p(\eta)$ she will identify the correct one $\hat{s}_i = \mathrm{sign}(\alpha_i)$. Eve's corrected outcomes are $\{\beta_i^E = \beta_i \cdot \hat{s}_i\}_{i=1}^N$, and her estimator $\hat{\phi}^E$ and MSE_E are analogous to those of Alice.

Therefore, in the CHECK phase Bob needs to ensure that Eve's estimation will be more noisy than Alice's. The degree to which this is true is defined as privacy:

$$\mathcal{P} = 1 - \frac{\mathrm{MSE}_A}{\mathrm{MSE}_E}. \tag{1}$$

Observe that $\mathcal{P} \in [0, 1]$ if $\mathrm{MSE}_E \geq \mathrm{MSE}_A$, and it attains its maximum when $\mathrm{MSE}_A/\mathrm{MSE}_E \to 0$, i.e., when Alice's error is vanishingly small with respect to that of Eve. In light of these reasons, given the measurement data $\{\beta_i\}_{i=1}^N$, Bob estimates the privacy (1) with the maximum-likelihood estimator $\hat{\mathcal{P}} = \mathcal{P}|_{\eta=\left|\frac{1}{N\alpha}\sum_{i=1}^N \beta_i^A\right|^2}$ and checks

whether it respects a predefined threshold, i.e., $\hat{\mathcal{P}} \geq 1-\epsilon$, where ϵ was previously agreed upon by Alice and Bob, also taking into account the uncertainties on the estimated privacy . If this holds true, then the check passes, otherwise the protocol is aborted, in line with DV protocols [3, 6, 12]. Note that, in the latter case, Eve will not be able to estimate the phase at all, since she does not have access to the measurement data.

MSE analysis – Bob's heterodyne outcome in round i can be written as $\beta_i = \sqrt{\eta}\, s_i\, \alpha + n_i$ where $n_i \sim \mathcal{CN}(0,1)$ iid, and $\mathcal{CN}(m,\sigma^2)$ denotes a circularly symmetric complex Gaussian random variable with mean m and variance σ^2. Alice forms the sign-aligned variables $\beta_i^A = r(\phi) + \tilde{n}_i$, where $r(\phi) = \sqrt{\eta}\,\alpha e^{\mathrm{i}\phi} > 0$ and $\tilde{n}_i \equiv s_i n_i \sim \mathcal{CN}(0,1)$, then she calculates the signed average $\bar{\beta}^A = \frac{1}{N}\sum_{i=1}^N \beta_i^A \sim \mathcal{CN}\Big(r(\phi), \frac{1}{N}\Big)$. Therefore, Alice's local MSE can be written as

$$\mathrm{MSE}_A(\phi) = \int_{\mathbb{C}} d^2 z\, (\theta-\phi)^2 p_{\bar{\beta}^A}(z|\phi), \tag{2}$$

where $p_{\bar{\beta}^A}(z|\phi) = \frac{N}{\pi}\exp\big(-N|z-r(\phi)|^2\big)$ is the probability density function of the signed average and $\theta = \arg z$ is the value of the estimator $\hat{\phi}^A$ when $\bar{\beta}^A = z$. Now, let us note that $\mathrm{MSE}_A(\phi)$ depends only on the difference $\theta-\phi$, up to an irrelevant global-phase change in the exponent of $p_{\bar{\beta}^A}(z|\phi)$; as a consequence, the local MSE is independent of the phase ϕ to be estimated and it equals the average MSE. We conclude that the estimator's performance is the same both in the local and Bayesian setting, independently of the prior, and is given by (2) with $\phi = 0$. Finally, by setting $z = \rho e^{\mathrm{i}\theta}$ and carrying out the radial integral we obtain $\mathrm{MSE}_A = \int_{-\pi}^{\pi} d\theta\, \theta^2 p_{\hat{\phi}}(\theta; r)$, with

$$\begin{aligned} p_{\hat{\phi}}(\theta;r) = \frac{1}{2\pi} e^{-Nr^2} \\ \cdot \Big[1 + \sqrt{\pi N} r\cos\theta\; e^{N(r\cos\theta)^2}\; \Big(1+\mathrm{Erf}(\sqrt{N} r\cos\theta)\Big)\Big] \end{aligned} \tag{3}$$

the posterior probability density of Alice's estimator, $r = r(0)$, and Erf(x) the error function, as shown in the SM. Interestingly, note that, since (3) is an even function of θ, the estimator is unbiased for any N.

Similarly, Eve's sign-aligned variables can be written as $\beta_i^E = \hat{s}_i\beta_i = D_i r(\phi) + \tilde{n}_i$, where $\tilde{n}_i \sim \mathcal{CN}(0,1)$, $D_i = \hat{s}_i s_i \in \{\pm 1\}$ and $\Pr(D_i = -1) = p(\eta)$; hence their probability density is a mixture of Gaussians weighted by the Helstrom probabilities $p(\eta)$, $q(\eta)$. As shown in the SM via the characteristic function, the probability density of Eve's signed average, $\bar{\beta}^E \equiv \frac{1}{N}\sum_{i=1}^N \beta_i^E$, is also a mixture of Gaussians with binomial weights:

$$p_{\bar{\beta}_E}(z|\phi) = \mathbb{E}_{k\sim\mathrm{Bin}(N,p(\eta))} \exp\Big(-N\,\Big|z - r(\phi)\Big(1-\frac{2k}{N}\Big)\Big|^2\Big), \tag{4}$$

where $\mathrm{Bin}(N,p(\eta))$ is the binomial distribution of the number of errors k in N discrimination experiments with single-error probability $p(\eta)$. We conclude that, as in Alice's case, Eve's local MSE is ϕ-independent and therefore equal to the average MSE:

$$\mathrm{MSE}_E = \mathbb{E}_{k\sim\mathrm{Bin}(N,p(\eta))}\mathrm{MSE}_A\big|_{r\mapsto r_k}. \tag{5}$$

Interestingly, (5) shows that Eve's MSE can be expressed as a binomial expectation of the MSE that Alice would have if she started with a different coherent-state amplitude $r_k = \sqrt{\eta}\,\alpha(1-\frac{2k}{N})$; indeed, the latter corresponds to Eve's observed average amplitude over the N rounds, when she commits exactly k discrimination errors.

Asymptotic performance – In the large-N limit, we can obtain analytical expressions for the MSE's and the privacy parameter by linearizing the estimator and approximating the binomial distribution with a Gaussian. Indeed, Eve's MSE can be written as an expectation over three random variables, obtained via averaging of Eve's data: $\mathrm{MSE}_E = \mathbb{E}\arg^2(r\bar{D} + X + \mathrm{i}Y)$, where $\bar{D} = \frac{1}{N}\sum_{i=1}^N D_i$ is binomial-distributed, while X and Y are the real and imaginary parts of the complex-normal-distributed random variable $\frac{1}{N}\sum_{i=1}^N \tilde{n}_i$. Expanding the arg function to the second order, we obtain

$$\mathrm{MSE}_E = \mathbb{E}\left[\left(\frac{Y}{r\bar{D}+X}\right)^2 - \frac{2}{3}\left(\frac{Y}{r\bar{D}+X}\right)^4\right] + O(N^{-3}). \tag{6}$$

Since the three variables are independent, the expectation with respect to Y can be carried out straightforwardly. Instead, the expectation of the quantities in the denominator can be approximated via a Taylor series of the probability distribution, also known as Edgeworth expansion [31], obtaining (see SM):

$$\mathrm{MSE}_E \sim \frac{1}{2N\,r^2(1-2p(\eta))^2}\left(1 + \frac{1+24r^2p(\eta)(1-p(\eta))}{4N\,r^2(1-2p(\eta))^2}\right) \tag{7}$$

up to $O(N^{-3})$, which characterizes the precision beyond the usual asymptotic assessment based on the Cramér-Rao bound. Note that Alice's MSE can be recovered in the same limit by setting $p(\eta) = 0$ above, i.e.,

$$\mathrm{MSE}_A \sim \frac{1}{2N\,r^2}\left(1 + \frac{1}{4N\,r^2}\right). \tag{8}$$

Therefore, the privacy behaves asymptotically as

$$\mathcal{P} \sim 1 - (1-2p(\eta))^2\left(1 - \frac{(6r^2+1)p(\eta)(1-p(\eta))}{N\,r^2(1-2p(\eta))^2}\right) \tag{9}$$

up to $O(N^{-2})$. In particular, as $N\to\infty$ the privacy tends to $\mathcal{P}_\infty = \exp\big(-4\alpha^2(1-\eta)\big)$ for finite α. Furthermore, since we now have an analytical expression $\mathcal{P}_\infty(\eta)$, a monotonic function of η, in the large-N limit a threshold on the privacy can be established in terms of a confidence interval. Namely, Alice and Bob can easily choose a threshold ϵ and a confidence interval δ such that $\Pr(\mathcal{P}_\infty(\eta) \geq 1-\epsilon|\{\beta_i\}_{i=1}^N) \equiv \Pr(\eta \geq \eta(\epsilon)|\{\beta_i\}_{i=1}^N) \geq 1-\delta$.

We conclude the asymptotic analysis by observing that the minimum MSE attainable with coherent-state probes

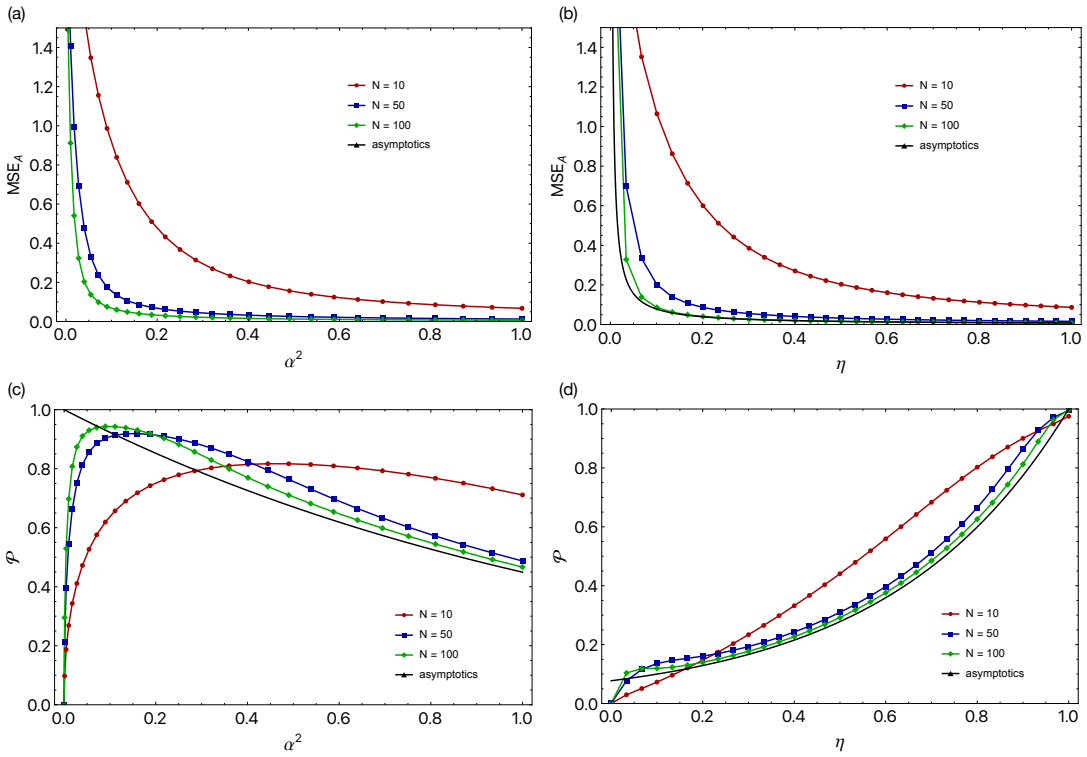

Figure 2: Plots of the finite-size and first-order asymptotic ($N = 100$) behaviour of the estimation error MSE_A (a,b) and privacy $\mathcal{P}$ (c,d), as a function of the initial probes' mean-photon number α^2 (a,c) and channel transmissivity η.

scales, for large N, as $\mathrm{MSE}_A/2$, and the optimal measurement is homodyne [30], aligned orthogonally to the initial coherent-state phase. Note however that Alice and Bob need to estimate also the loss η, hence the estimation performance has to be evaluated in a multi-parameter setting, which does not allow for optimising the uncertainties on individual parameters. Nevertheless, previous works point to the optimality of coherent-states and heterodyne measurements for the joint phase- and amplitude- estimation with single-mode probes [32]. Furthermore, the use of non-binary constellations will immediately favour heterodyne over homodyne.

Finite-size behaviour – The previously obtained MSE and privacy expressions can be studied numerically for any finite N, providing a full characterization of the protocol's performance in the finite-size regime. In Fig. 2 we plot Alice's MSE and the privacy as a function of the probe's mean-photon number and the channel transmissivity. We observe that MSE_A decreases both with α^2 and η; similarly, $\mathcal{P}$ increases with η. This can be understood since in all three cases the figure of merit is enhanced by a larger received probe mean-photon number. On the other hand, it appears that, for any finite N, there exists an optimum value of α^2 that maximizes the estimation privacy. This is due to the trade-off between decreasing MSE_A, which requires large α^2, and decreasing $\mathrm{MSE}_A/\mathrm{MSE}_E$, which requires small α^2. Below a certain threshold number of photons, the higher noise experienced by Eve cannot compensate for the decrease in estimation error experienced by Alice. Furthermore, we note that for large photon number the asymptotic expression is already valid at moderate $N > 50$. However, the approximation breaks down for sufficiently small energy, where a more careful expansion at fixed $N\alpha^2$ should be undertaken to analyze the small-α behaviour, using similar methods as above.

Conclusions – We have introduced and fully characterized the first single-user CV-RPQS protocol under the assumption of passive photon-splitting attacks. This allowed us to derive analytical results with the use of a discrete-modulation, usually hard to tackle, by bounding the attacker's discrimination capabilities. We studied both the asymptotic and finite-size regime, introducing the concept of estimation privacy and studying its connection with the estimation error. Our results show that, for finite number of rounds, there is an optimal probe mean-photon number that ensures the highest privacy while maintaining good estimation performance, similarly to the optimal modulation of GG02. Our work illustrates the merits of inspecting technologically relevant specific attacks for more stringent bounds in PRQS.

Acknowledgements – We thank Gabriele Bizzarri for useful discussions on PQRS. M.R. acknowledges support from the project PNRR -Id MSCA 0000011-SQUID-CUP F83C22002390007 (Young Researchers) - Finanzi-

ato dall'UE - NextGeneration EU. This work has been realised with the support of the PRIN project PRIN22-RISQUE-2022T25TR3 of the Italian Ministry of University. M.B. acknowledges support by Rome Technopole Innovation Ecosystem (PNRR grant M4-C2-Inv) and MUR Dipartimento di Eccellenza 2023-2027.

A Full derivation of the MSE for BPSK alphabet

We consider the protocol described in the main text with a BPSK alphabet $\{\pm\alpha : \alpha > 0\}$. As we have already shown that the MSE is ϕ-invariant, without loss of generality we align the axis so that the unknown phase is $\phi = 0$, and let $\alpha_i = s_i\alpha$ with $s_i \in \{+1, -1\}$. Bob's heterodyne outcome in round i is modeled as

$$\beta_i = \sqrt{\eta}\, s_i\, \alpha + n_i, \qquad n_i \sim \mathcal{CN}(0,1) \text{ i.i.d.}, \tag{10}$$

where $\mathcal{CN}(m, \sigma^2)$ denotes a circularly symmetric complex Gaussian random variable with mean m and variance σ^2, i.e.

$$p_Z(z) = \frac{1}{\pi\sigma^2} \exp\!\left(-\frac{|z-m|^2}{\sigma^2}\right), \qquad z \in \mathbb{C}. \tag{11}$$

In this notation, $\mathrm{Re}(Z)$ and $\mathrm{Im}(Z)$ are independent real Gaussian variables, each with mean $\mathrm{Re}(m)$ and $\mathrm{Im}(m)$ respectively, and variance $\sigma^2/2$.

A.1 Alice's MSE

Alice forms the sign-aligned variables

$$\beta_i^A \equiv s_i\beta_i = r + \tilde{n}_i, \qquad r \equiv \sqrt{\eta}\,\alpha > 0, \quad \tilde{n}_i \equiv s_i n_i \sim \mathcal{CN}(0,1). \tag{12}$$

The signed average is

$$\bar{\beta}^A \equiv \frac{1}{N}\sum_{i=1}^{N} \beta_i^A \;\sim\; \mathcal{CN}\Big(r, \frac{1}{N}\Big). \tag{13}$$

then Alice's estimator for the phase is $\hat{\phi}_A = \arg(\bar{\beta}^A)$. Next, we compute the mean square error (MSE) of the estimator.

Since $\bar{\beta}^A \sim \mathcal{CN}(r, 1/N)$ with $r = \sqrt{\eta}\,\alpha > 0$, its pdf is

$$p_{\bar{\beta}^A}(z) = \frac{N}{\pi} \exp\big(-N|z-r|^2\big), \qquad z \in \mathbb{C}. \tag{14}$$

Write $z = \rho e^{i\theta}$ with $\rho \geq 0$, $\theta \in (-\pi, \pi]$ and Jacobian $\mathrm{d}x\,\mathrm{d}y = \rho\,\mathrm{d}\rho\,\mathrm{d}\theta$. Then

$$p_{\hat{\phi}_A}(\theta) = \int_0^\infty p_{\bar{\beta}^A}(\rho e^{i\theta})\,\rho\,\mathrm{d}\rho = \int_0^\infty \frac{N}{\pi} \exp\big(-N(\rho^2 + r^2 - 2r\rho\cos\theta)\big)\,\rho\,\mathrm{d}\rho, \tag{15}$$

and the mean-squared error of the phase estimator $\hat{\phi}_A = \arg(\bar{\beta}^A)$ is

$$\mathrm{MSE}_A = \int_{-\pi}^{\pi} \theta^2\, p_{\hat{\phi}_A}(\theta)\,\mathrm{d}\theta. \tag{16}$$

The radial integral in (15) can be evaluated in closed form by completing the square. Let $\kappa \equiv Nr^2 = N\eta\alpha^2$, then we have

$$p_{\hat{\phi}_A}(\theta) = \frac{1}{\pi} e^{-\kappa} \int_0^\infty d\rho\,\rho \exp\big(-\rho^2 + 2\sqrt{\kappa}\rho\cos\theta\big) = \frac{1}{\pi} e^{-\kappa\sin^2\theta} \int_0^\infty d\rho\,\rho \exp\big(-(\rho - \sqrt{\kappa}\cos\theta)^2\big) \tag{17}$$

$$= \frac{1}{\pi} \int_{-\sqrt{\kappa}\cos\theta}^{\infty} e^{-t^2} \Big(t + \sqrt{\kappa}\,\cos\theta\Big)\,\mathrm{d}t = \frac{1}{2\pi} e^{-\kappa\sin^2\theta} \left(e^{-\kappa\cos^2\theta} + \sqrt{\pi\kappa}\cos\theta(1 + \mathrm{Erf}(\sqrt{\kappa}\cos\theta))\right), \tag{18}$$

which matches the expression of $p_{\hat{\phi}}(\theta; r)$ in the main text.

A.2 Eve's MSE

Eve performs a Helstrom test on her environmental mode. Let

$$P_e^{\mathrm{Hel}} = \tfrac{1}{2}\Big(1 - \sqrt{1 - e^{-4(1-\eta)\alpha^2}}\Big), \qquad r = \sqrt{\eta}\,\alpha > 0, \qquad p = P_e^{\mathrm{Hel}}, \quad q = 1 - p.$$

where we omit the dependence of the probabilities on η. With Eve's decision $\hat{s}_i \in \{\pm 1\}$ and $D_i = \hat{s}_i s_i \in \{\pm 1\}$, the corrected public data is

$$\beta_i^E = \hat{s}_i\beta_i = D_i r + \tilde{n}_i, \qquad \Pr(D_i = +1) = q,\ \Pr(D_i = -1) = p, \quad \tilde{n}_i \sim \mathcal{CN}(0,1), \tag{19}$$

so

$$p_{\beta_i^E}(z) = q\,\frac{1}{\pi}e^{-|z-r|^2} + p\,\frac{1}{\pi}e^{-|z+r|^2}. \tag{20}$$

Similar to Alice's case, Eve takes the sign-corrected average of Bob's public data

$$\bar{\beta}^E \equiv \frac{1}{N}\sum_{i=1}^{N}\beta_i^E, \tag{21}$$

and her estimator is $\hat{\phi}_E = \arg(\bar{\beta}^E)$. Therefore, We are interested in the probability distribution of $\bar{\beta}^E$. For this, we make use of the characteristic function of a two-variable probability distribution defined as $\phi_Z(u_x, u_y) = \mathbb{E}[e^{i(u_x X + u_y Y)}]$, where $Z = X + iY$ is our complex random variable. Therefore, in our case

$$\phi_{\beta_i^E}(u_x, u_y) = e^{-\frac{1}{4}(u_x^2+u_y^2)}\Big[q\,e^{iru_x} + p\,e^{-iru_x}\Big]. \tag{22}$$

As $\bar{\beta}^E$ is the average of N iid variables, using standard properties of the characteristic function we can write

$$\phi_{\bar{\beta}_E}(u_x, u_y) = \Big(\phi_{\beta_i}\big(\tfrac{u_x}{N}, \tfrac{u_y}{N}\big)\Big)^N = \exp\Big(-\frac{u_x^2+u_y^2}{4N}\Big)\Big[q\,e^{i\frac{r}{N}u_x} + p\,e^{-i\frac{r}{N}u_x}\Big]^N. \tag{23}$$

Expanding the power shows that $\bar{\beta}_E$ is a finite Gaussian mixture, with binomial coefficients:

$$p_{\bar{\beta}_E}(z) = \sum_{k=0}^{N}\binom{N}{k}q^{N-k}p^k\,\frac{N}{\pi}\exp\Big(-N\,|z-r_k|^2\Big), \qquad r_k = r\Big(1-\frac{2k}{N}\Big), \tag{24}$$

which can be written as an average of Alice's probability distribution (14) with different k-dependent mean:

$$p_{\bar{\beta}_E}(z) = \sum_{k=0}^{N}\mathrm{Bin}(k|N,p)\,p_{\bar{\beta}^A}(z)\Big|_{r\mapsto r_k}. \tag{25}$$

By linearity, from the previous calculation in Alice's case it then follows the result of the main text.

A.3 Optimality properties of the estimators

It is straightforward to show that Alice's chosen estimator is maximum-likelihood. Given the sign-aligned variables $\{\beta_i^A\}_{i=1}^N$ we can write their joint probability density as

$$p_{\{\beta_i^A\}_{i=1}^N}(z_1, \cdots, z_N) = \frac{1}{(\pi\sigma)^N}\exp\left(-\frac{1}{\sigma^2}\sum_{i=1}^{N}|z_i - re^{\mathrm{i}\phi}|^2\right) \tag{26}$$

and we can write the log-likelihood function (for flat prior) as

$$\ell(\phi|z_1, \cdots, z_N) \propto -\sum_{i=1}^{N}(|z_i|^2 + r^2 - 2r\,\mathrm{Re}\{z_i e^{-\mathrm{i}\phi}\}) = \text{const.} + 2r\left|\sum_i z_i\right|\cos\left(\phi - \arg\sum_i z_i\right). \tag{27}$$

Setting its derivative with respect to ϕ equal to zero we obtain the value of our estimator:

$$\hat{\phi}_{\mathrm{ml}} = \arg\sum_{i=1}^{N} z_i \equiv \arg\frac{1}{N}\sum_{i=1}^{N} z_i. \tag{28}$$

As a by-product, we also obtain the joint maximum-likelihood estimator for r, hence for the transmissivity:

$$\hat{\eta} = \left|\frac{1}{N\alpha}\sum_{i=1}^{N} z_i\right|^2. \tag{29}$$

Finally, since $\mathcal{P}(\eta)$ is a deterministic function, a maximum-likelihood estimator for $\mathcal{P}$ is exactly $\hat{\mathcal{P}} = \mathcal{P}(\hat{\eta})$.

B Large-N limit

We recall that Eve forms the corrected average

$$\bar{\beta}^E \;=\; \frac{1}{N}\sum_{i=1}^{N}\beta_i^E \;=\; \frac{1}{N}\sum_{i=1}^{N}\big(D_i\, r+\tilde{n}_i\big) \;=\; r\,\bar{D} \;+\; \bar{n}, \qquad r\equiv\sqrt{\eta}\,\alpha>0. \tag{30}$$

Hence $\bar{n}\sim\mathcal{CN}(0,1/N)$ and

$$\bar{D} \;\equiv\; \frac{1}{N}\sum_{i=1}^{N}D_i, \qquad \mathbb{E}[D_i]=1-2p, \quad \mathrm{Var}(D_i)=4p(1-p). \tag{31}$$

Eve'ss estimator is $\hat{\phi}_E=\arg(\bar{\beta}^E)$, and we wish to compute

$$\mathrm{MSE}_E \;\equiv\; \mathbb{E}\big[\hat{\phi}_E^{\,2}\big] \tag{32}$$

for large N.

B.1 Small-angle linearization at large N.

Write $\bar{n}=X+iY$ with $X,Y\sim\mathcal{N}(0,\frac{1}{2N})$ independent, and note that $\bar{\beta}^E=r\bar{D}+X+iY$. Then the estimator can be expressed as

$$\hat{\phi}_E \;=\; \arg(r\bar{D}+X+iY) \;=\; \arctan\frac{Y}{r\bar{D}+X}. \tag{33}$$

For large N, $X,Y=O(N^{-1/2})$, while $\bar{D}=O(1)$, hence we may expand the arctangent around zero as

$$\hat{\phi}_E \;=\; \frac{Y}{r\bar{D}+X} \;-\; \frac{1}{3}\left(\frac{Y}{r\bar{D}+X}\right)^3 \;+\; O\left(\left(\frac{Y}{r\bar{D}+X}\right)^5\right). \tag{34}$$

Now note that the three random variables are independent and, in particular, it holds $\mathbb{E}[Y]=0$, $\mathbb{E}[Y^2]=1/(2N)$ and $\mathbb{E}[Y^4]=3/(4N^2)$, hence

$$\mathrm{MSE}_E \;=\; \mathbb{E}\big[\hat{\phi}_E^{\,2}\big]=\frac{1}{2N}\,\mathbb{E}\left[\frac{1}{(r\bar{D}+X)^2}\right]-\frac{1}{2N^2}\,\mathbb{E}\left[\frac{1}{(r\bar{D}+X)^4}\right] \;+\; O(N^{-3}). \tag{35}$$

B.2 Edgeworth (delta) expansion

Let $\{W_i\}_{i=1}^N$ be i.i.d. random variables with mean $\mu=\mathbb{E}[W_i]$, variance $\sigma^2=\mathrm{Var}(W_i)$, and higher cumulants κ_3,κ_4, etc. For the sample mean

$$\bar{W} \;=\; \frac{1}{N}\sum_{i=1}^{N}W_i,$$

we have the cumulant scalings

$$\kappa_1(\bar{W})=\mu, \qquad \kappa_2(\bar{W})=\frac{\sigma^2}{N},$$

Then for any sufficiently smooth test function g, the Edgeworth (or delta-method) expansion of the expectation of $g(\bar{W})$ around μ is [31]

$$\mathbb{E}\big[g(\bar{W})\big]=g(\mu)+\frac{1}{2}\,g''(\mu)\,\frac{\sigma^2}{N}+O\big(N^{-2}\big)\,. \tag{36}$$

Here, the first term is the mean value $g(\mu)$, while the second one captures Gaussian fluctuations, and all higher cumulant contributions are contained in the remainder $O(N^{-2})$.

We now let

$$\bar{W} \;\equiv\; r\,\bar{D}+X \;=\; \frac{1}{N}\sum_{i=1}^{N}W_i, \qquad W_i \;\coloneqq\; rD_i+X_i, \tag{37}$$

where $X_i\sim\mathcal{N}(0,\frac{1}{2})$ are iid and independent of D_i. Then, the random variables W_i have the following cumulants:

$$\mu \;\equiv\; \mathbb{E}[W_i] \;=\; r(1-2p), \tag{38}$$

$$\sigma^2 \;\equiv\; \mathrm{Var}(W_i) \;=\; 4r^2p(1-p)+\tfrac{1}{2}, \tag{39}$$

while higher cumulants will not be needed.

Using (36) with $g_k(u) = u^{-k}$, whose second derivative is $g_k''(u) = k(k+1)u^{-(k+2)}$, we find, for $k = 2$ and $k = 4$,

$$\mathbb{E}\left[\frac{1}{\bar{W}^{\,2}}\right] = \mu^{-2} + \frac{3\sigma^2}{N}\,\mu^{-4} - \frac{4\kappa_3}{N^2}\,\mu^{-5} + \frac{15\sigma^4}{N^2}\,\mu^{-6} + O(N^{-3}), \tag{40}$$

$$\mathbb{E}\left[\frac{1}{\bar{W}^{\,4}}\right] = \mu^{-4} + \frac{10\sigma^2}{N}\mu^{-6} + O\left(\frac{1}{N^2}\right). \tag{41}$$

B.3 Final large-N expansion of MSE

Recalling (35), we obtain

$$\mathrm{MSE}_E \;=\; \frac{1}{2N}\,\mathbb{E}\left[\frac{1}{\bar{W}^{\,2}}\right] \;-\; \frac{1}{2N^2}\,\mathbb{E}\left[\frac{1}{\bar{W}^{\,4}}\right] + O(N^{-3}). \tag{42}$$

Substituting the expansions (40), (41) yields

$$\mathrm{MSE}_E \;=\; \frac{1}{2N}\,\frac{1}{\mu^2} \;+\; \frac{1}{2N^2}\,\frac{3\sigma^2 - 1}{\mu^4} \;+\; O\big(N^{-3}\big)\,. \tag{43}$$

Equivalently, in terms of (r, p),

$$\mathrm{MSE}_E \;=\; \frac{1}{2N\,r^2(1-2p)^2} \;+\; \frac{6r^2p(1-p) + \frac{1}{4}}{N^2\,r^4(1-2p)^4} \;+\; O\big(N^{-3}\big)\,. \tag{44}$$

References

[1] Stephanie Wehner, David Elkouss, and Ronald Hanson. Quantum internet: A vision for the road ahead. Science (80-.)., 362(6412):eaam9288, oct 2018.

[2] Peter P. Rohde, Zixin Huang, Yingkai Ouyang, He-Liang Huang, Zu-En Su, Simon Devitt, Rohit Ramakrishnan, Atul Mantri, Si-Hui Tan, Nana Liu, Scott Harrison, Chandrashekar Radhakrishnan, Gavin K. Brennen, Ben Q. Baragiola, Jonathan P. Dowling, Tim Byrnes, and William J. Munro. The Quantum Internet (Technical Version). jan 2025.

[3] Zixin Huang, Chiara Macchiavello, and Lorenzo Maccone. Cryptographic quantum metrology. Phys. Rev. A, 99(2):022314, feb 2019.

[4] Yuki Takeuchi, Yuichiro Matsuzaki, Koichiro Miyanishi, Takanori Sugiyama, and William J. Munro. Quantum remote sensing with asymmetric information gain. Phys. Rev. A, 99(2):022325, feb 2019.

[5] Peng Yin, Yuki Takeuchi, Wen-Hao Zhang, Zhen-Qiang Yin, Yuichiro Matsuzaki, Xing-Xiang Peng, Xiao-Ye Xu, Jin-Shi Xu, Jian-Shun Tang, Zong-Quan Zhou, Geng Chen, Chuan-Feng Li, and Guang-Can Guo. Experimental Demonstration of Secure Quantum Remote Sensing. Phys. Rev. Appl., 14(1):014065, jul 2020.

[6] Nathan Shettell, Elham Kashefi, and Damian Markham. Cryptographic approach to quantum metrology. Phys. Rev. A, 105(1):L010401, jan 2022.

[7] Sean William Moore and Jacob Andrew Dunningham. Secure quantum remote sensing without entanglement. AVS Quantum Sci., 5(1), mar 2023.

[8] Wenjie He, Chunfeng Huang, Rui Guan, Ye Chen, Zhenrong Zhang, and Kejin Wei. Experimental secure entanglement-free quantum remote sensing over 50 km of optical fiber, dec 2024.

[9] Joseph Ho, Jonathan W. Webb, Russell M. J. Brooks, Federico Grasselli, Erik Gauger, and Alessandro Fedrizzi. Quantum-private distributed sensing, oct 2024.

[10] Majid Hassani, Santiago Scheiner, Matteo G. A. Paris, and Damian Markham. Privacy in networks of quantum sensors. aug 2024.

[11] Luís Bugalho, Majid Hassani, Yasser Omar, and Damian Markham. Private and Robust States for Distributed Quantum Sensing. jan 2025.

[12] G. Bizzarri, M. Barbieri, M. Manrique, M. Parisi, F. Bruni, I. Gianani, and M. Rosati. Faithful and secure distributed quantum sensing under general-coherent attacks. may 2025.

[13] Jarn de Jong, Santiago Scheiner, Naomi R. Solomons, Ziad Chaoui, Damian Markham, and Anna Pappa. Anonymous and private parameter estimation in networks of quantum sensors. jul 2025.

[14] Uesli Alushi and Roberto Di Candia. Privacy in Distributed Quantum Sensing with Gaussian Quantum Networks. sep 2025.

[15] A. de Oliveira Junior, Anton L. Andersen, Benjamin Lundgren Larsen, Sean William Moore, Damian Markham, Masahiro Takeoka, Jonatan Bohr Brask, and Ulrik L. Andersen. Privacy in continuous-variable distributed quantum sensing. sep 2025.

[16] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In Proc. IEEE Int. Conf. Comput. Syst. Signal Process., page 8, New York, 1984.

[17] Artur K. Ekert. Quantum cryptography based on Bell's theorem. Phys. Rev. Lett., 67(6):661–663, aug 1991.

[18] Frédéric Grosshans and Philippe Grangier. Continuous Variable Quantum Cryptography Using Coherent States. Phys. Rev. Lett., 88(5):4, 2002.

[19] Shouvik Ghorai, Philippe Grangier, Eleni Diamanti, and Anthony Leverrier. Asymptotic Security of Continuous-Variable Quantum Key Distribution with a Discrete Modulation. Phys. Rev. X, 9(2):021059, jun 2019.

[20] Jie Lin, Twesh Upadhyaya, and Norbert Lütkenhaus. Asymptotic Security Analysis of Discrete-Modulated Continuous-Variable Quantum Key Distribution. Phys. Rev. X, 9(4):041064, dec 2019.

[21] Aurélie Denys, Peter Brown, and Anthony Leverrier. Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. Quantum, 5:540, sep 2021.

[22] Florian Kanitschar, Ian George, Jie Lin, Twesh Upadhyaya, and Norbert Lütkenhaus. Finite-Size Security for Discrete-Modulated Continuous-Variable Quantum Key Distribution Protocols. PRX Quantum, 4(4):040306, oct 2023.

[23] Matteo Rosati, Giacomo De Palma, Andrea Mari, and Vittorio Giovannetti. Optimal quantum state discrimination via nested binary measurements. Phys. Rev. A - At. Mol. Opt. Phys., 95(4):1–10, 2017.

[24] M. Bilkis, M. Rosati, R. Morral Yepes, and J. Calsamiglia. Real-time calibration of coherent-state receivers: Learning by trial and error. Phys. Rev. Res., 2(3):033295, aug 2020.

[25] M. Bilkis, Matteo Rosati, and John Calsamiglia. Reinforcement-learning calibration of coherent-state receivers on variable-loss optical channels. In 2021 IEEE Inf. Theory Work., pages 1–6. IEEE, oct 2021.

[26] Matteo Rosati and Albert Solana. Joint-detection learning for optical communication at the quantum limit. Opt. Quantum, 2(6):390, dec 2024.

[27] Matteo Rosati and Gabriella Cincotti. A Fourier machine for quantum optical communications. J. Light. Technol., pages 1–8, 2025.

[28] Farzad Kianvash and Matteo Rosati. Probabilistic pulse-position modulation for classical communication on quantum channels. Phys. Rev. A, 112(3):032624, sep 2025.

[29] Michele N. Notarnicola, Stefano Olivares, Enrico Forestieri, Emanuele Parente, Luca Potí, and Marco Secondini. Probabilistic amplitude shaping for continuous-variable quantum key distribution with discrete modulation over a wiretap channel. IEEE Transactions on Communications, 72(1):375–386, 2024.

[30] Carl W Helstrom. Quantum Detection and Estimation Theory, volume 84. Academic press, New York, 1976.

[31] John E. Kolassa. Series Approximation Methods in Statistics, volume 88 of Lecture Notes in Statistics. Springer New York, 2006.

[32] M. G. Genoni, M. G. A. Paris, G. Adesso, H. Nha, P. L. Knight, and M. S. Kim. Optimal estimation of joint parameters in phase space. jan 2013.