

Private Remote Phase Estimation over a Lossy Quantum Channel

Farzad Kianvash,¹ Marco Barbieri^{2,3,4} and Matteo Rosati¹

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 Fiorentino 50019, Florence, Italy*

⁴*INFN, Sezione di Roma Tre, Via Della Vasca Navale 84, 00146 Rome, Italy*



(Received 12 November 2025; accepted 21 January 2026; published 11 February 2026)

Private remote quantum sensing 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 analyze a private remote sensing protocol 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.

DOI: [10.1103/rhgw-t21z](https://doi.org/10.1103/rhgw-t21z)

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 sensing by private quantum remote resources (SPQR), a technique that allows a quantum provider to estimate physical quantities at a distant location, connected via an insecure quantum communication channel [3–12], 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.

The SPQR problem has been well studied using discrete variable (DV) states in the single-user setting [3–9,12],

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 multiuser distributed sensing, research has focused on guaranteeing privacy with respect to other users rather than to an eavesdropper [10,11,13–15]. 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 endeavor 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 SPQR 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. Extending these approaches to continuous variables (CVs) is made more critical by their reliance on fidelity as a figure of merit, which is loose by itself [16], as well as on bounded observables. Pursuing an analogy with secure communications, insight in such cases is gained by inspecting specific attack models.

In this Letter, 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

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

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 Letter, to the best of our knowledge, pioneers SPQR protocols based on continuous-variable (CV) states in the single-user setting (for the distinct multiuser setting, see instead the very recent Refs. [14,15]). Similarly to the DV case where SPQR schemes are based on seminal QKD protocols such as BB84 and E91 [17,18], our proposed CV protocol is reminiscent of GG02 [19]. However, in order to provide a realistic protocol and avoid oversimplifications connected with a continuous signal distribution, at variance with GG02, we consider a discrete constellation of probe states [20–23]. 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 [24–29] 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, $|\alpha\rangle_i = e^{a^\dagger \alpha_i - a \alpha_i^\dagger} |0\rangle$, 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., $\alpha_i \in \mathcal{A} = \{\alpha e^{i\theta_k} : \alpha > 0\}_{k=1}^A$. 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 $\{(1/\pi)|\beta\rangle\langle\beta|\}_{\beta \in \mathbb{C}}$, 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 SPQR 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.

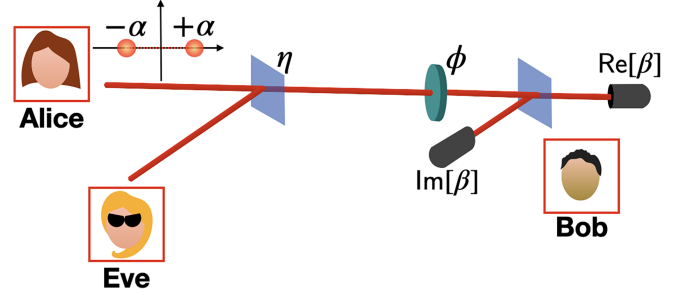


FIG. 1. Schematic depiction of our SPQR protocol. Alice wants to estimate a phase ϕ at Bob’s location, out of her reach. She thus delegates the measurement to Bob, who performs heterodyne measurements on the transmitted probes. Eve compromises the security of the protocol by tapping part of the signal,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

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 [25,29,30]. While this compromises the Gaussianity of the overall state, hence requiring greater care in secret key analysis [22,23], we will show how our SPQR 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 $s_i = \text{sign}(\alpha_i)$; then, she estimates the phase via the estimator $\hat{\phi}^A = \arg(1/N \sum_{i=1}^N \beta_i^A)$, which is maximum likelihood, as shown in the Supplemental Material (SM) [31]. 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., $\text{MSE}_A(\phi) = \mathbb{E}_{\{\beta_i^A\}|\phi}(\hat{\phi}^A - \phi)^2$; instead, in the Bayesian setting one studies the average MSE with respect to the phase distribution—i.e., $\text{MSE}_A = \mathbb{E}_\phi \text{MSE}_A(\phi)$. 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 [25]. Eve’s error is then quantified by the Helstrom bound [25,32]: $P_e^{\text{Hel}} = \frac{1}{2}(1 - \sqrt{1 - e^{-4(1-\eta)\alpha^2}})$; i.e., with probability $p(\eta) = P_e^{\text{Hel}}$, Eve will identify the wrong phase $\hat{s}_i = -\text{sign}(\alpha_i)$, while with probability $q(\eta) = 1 - p(\eta)$, she will identify the correct one $\hat{s}_i = \text{sign}(\alpha_i)$. 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:

$$\mathcal{P} = 1 - \frac{\text{MSE}_A}{\text{MSE}_E}. \quad (1)$$

Observe that $\mathcal{P} \in [0, 1]$ if $\text{MSE}_E \geq \text{MSE}_A$, and it attains its maximum when $\text{MSE}_A/\text{MSE}_E \rightarrow 0$ —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 [Eq. (1)] with the maximum-likelihood estimator $\hat{\mathcal{P}} = \mathcal{P}|_{\eta=(1/N\alpha)\sum_{i=1}^N|\beta_i^A|^2}$ 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 $n_i \sim \mathcal{CN}(0, 1)$ independent and identically distributed, 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 $r(\phi) = \sqrt{\eta}\alpha e^{i\phi} > 0$ and $\tilde{n}_i \equiv s_i n_i \sim \mathcal{CN}(0, 1)$, and then she calculates the signed average $\bar{\beta}^A = (1/N)\sum_{i=1}^N \beta_i^A \sim \mathcal{CN}(r(\phi), (1/N))$. Therefore, Alice's local MSE can be written as

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

where $p_{\bar{\beta}^A}(z|\phi) = (N/\pi) \exp(-N|z - r(\phi)|^2)$ 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 $\text{MSE}_A(\phi)$ 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 in both the local and the Bayesian setting, independently of the prior, and is given by Eq. (2) with $\phi = 0$. Finally, by setting $z = \rho e^{i\theta}$ and carrying out the radial integral, we obtain $\text{MSE}_A = \int_{-\pi}^{\pi} d\theta \theta^2 p_{\hat{\phi}}(\theta; r)$, with

$$p_{\hat{\phi}}(\theta; r) = \frac{1}{2\pi} e^{-Nr^2} \cdot [1 + \sqrt{\pi N} r \cos \theta e^{N(r \cos \theta)^2} (1 + \text{Erf}(\sqrt{N} r \cos \theta))] \quad (3)$$

as the posterior probability density of Alice's estimator, $r = r(0)$, and $\text{Erf}(x)$ being the error function, as shown in the SM [31]. Interestingly, note that, since Eq. (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 $\text{Pr}(D_i = -1) = p(\eta)$; hence, their probability density is a mixture of Gaussians weighted by the Helstrom probabilities $p(\eta)$, $q(\eta)$. As shown in the SM [31] via the characteristic function, the probability density of Eve's signed average, $\bar{\beta}^E \equiv (1/N)\sum_{i=1}^N \beta_i^E$, is also a mixture of Gaussians with binomial weights:

$$p_{\bar{\beta}^E}(z|\phi) = \mathbb{E}_{k \sim \text{Bin}(N, p(\eta))} \exp\left(-N \left|z - r(\phi) \left(1 - \frac{2k}{N}\right)\right|^2\right), \quad (4)$$

where $\text{Bin}(N, p(\eta))$ 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:

$$\text{MSE}_E = \mathbb{E}_{k \sim \text{Bin}(N, p(\eta))} \text{MSE}_A|_{r \rightarrow r_k}. \quad (5)$$

Interestingly, Eq. (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 $r_k = \sqrt{\eta}\alpha[1 - (2k/N)]$; 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 MSEs 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 the averaging of Eve's data: $\text{MSE}_E = \mathbb{E} \arg^2(r\bar{D} + X + iY)$, where $\bar{D} = (1/N)\sum_{i=1}^N D_i$ is binomial-distributed, while X and Y are the real and imaginary parts of the complex-normal-distributed random variable $(1/N)\sum_{i=1}^N \tilde{n}_i$. Expanding the arg function to the second order, we obtain

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

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 [33], obtaining (see the SM [31])

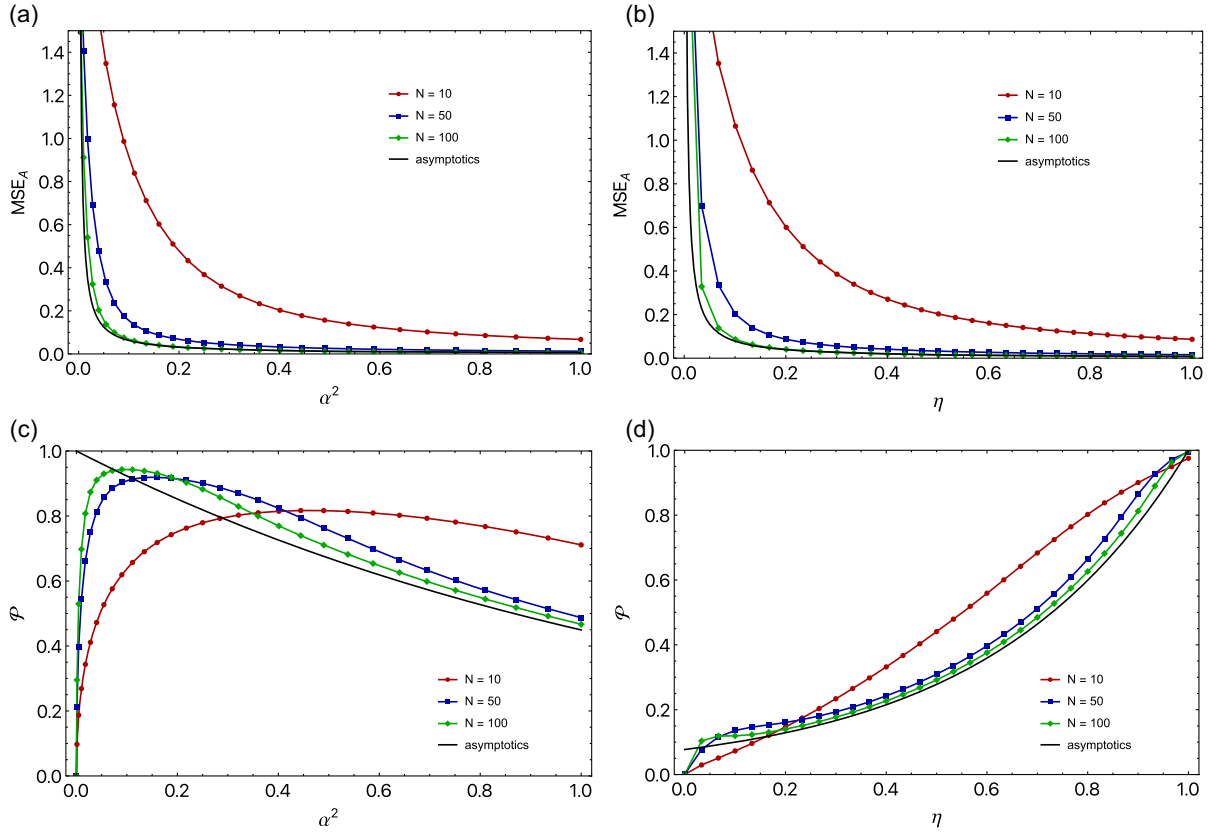


FIG. 2. Plots of the finite-size and first-order asymptotic ($N = 100$) behavior of (a),(b) the estimation error MSE_A and (c),(d) privacy $\mathcal{P}$, as a function of (a),(c) the initial probes' mean-photon number α^2 for fixed $\eta = 0.8$ and (b),(d) channel transmissivity η for fixed $\alpha = 0.8$.

$$\text{MSE}_E \sim \frac{1}{2Nr^2(1-2p(\eta))^2} \left(1 + \frac{1+24r^2p(\eta)(1-p(\eta))}{4Nr^2(1-2p(\eta))^2} \right) \quad (7)$$

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.,

$$\text{MSE}_A \sim \frac{1}{2Nr^2} \left(1 + \frac{1}{4Nr^2} \right). \quad (8)$$

Therefore, the privacy behaves asymptotically as

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

up to $O(N^{-2})$. In particular, as $N \rightarrow \infty$, the privacy tends to $\mathcal{P}_\infty = \exp(-4\alpha^2(1-\eta))$ 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 $\Pr(\mathcal{P}_\infty(\eta) \geq 1 - \epsilon | \{\beta_i\}_{i=1}^N) \equiv \Pr(\eta \geq \eta(\epsilon) | \{\beta_i\}_{i=1}^N) \geq 1 - \delta$.

Note that the minimum MSE attainable with coherent-state probes scales, for large N , as $\text{MSE}_A/2$, and the optimal measurement is homodyne [32], 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 optimizing 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 [34]. Furthermore, the use of nonbinary constellations will immediately favour heterodyne over homodyne.

We conclude by noting that the loose bounds applicable to discrete-variable systems, introduced in Refs. [6,12] for general attacks, are not applicable to our setting, since our protocol employs heterodyne detection, whose measurement outcomes are unbounded and therefore violate the assumptions underlying those bounds. Rather than relying on unrealistic truncations for the application of such bounds, the assumption of passive attacks effectively imposes a realistic energy constraint on Eve's attacks.

Finite-size behavior—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 tradeoff between decreasing MSE_A , which requires large α^2 , and decreasing $\text{MSE}_A/\text{MSE}_E$, 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 a 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 behavior, using similar methods as above.

Conclusions—We have introduced and fully characterized the first single-user CV-SPQR 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 a 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 Letter illustrates the merits of inspecting technologically relevant specific attacks for more stringent bounds in SPQR. The design of the protocol around coherent states and classical modulations makes it possible to envision an experimental realization based on off-the-shelf equipment, benefiting from a similar complexity as quantum key distribution [36].

Acknowledgments—We thank Gabriele Bizzarri for useful discussions on SPQR. M.R. acknowledges support from the project PNRR—Id MSCA 0000011-SQUID—CUP F83C22002390007 (Young Researchers)—Finanziato dall'Unione Europea—NextGenerationEU. This work has been realized with the support of the PRIN project PRIN22-RISQUE-2022T25TR3 of the Italian Ministry of University. M.B. acknowledges support by the Rome Technopole Innovation Ecosystem (PNRR

Grant M4-C2-Inv) and MUR Dipartimento di Eccellenza 2023–2027.

Data availability—The data that support the findings of this article are openly available [35].

-
- [1] S. Wehner, D. Elkouss, and R. Hanson, Quantum internet: A vision for the road ahead, *Science* **362**, eaam9288 (2018).
 - [2] P. P. Rohde, Z. Huang, Y. Ouyang, H.-L. Huang, Z.-E. Su, S. Devitt, R. Ramakrishnan, A. Mantri, S.-H. Tan, N. Liu, S. Harrison, C. Radhakrishnan, G. K. Brennen, B. Q. Baragiola, J. P. Dowling, T. Byrnes, and W. J. Munro, The quantum internet (technical version), [arXiv:2501.12107](#).
 - [3] Z. Huang, C. Macchiavello, and L. Maccone, Cryptographic quantum metrology, *Phys. Rev. A* **99**, 022314 (2019).
 - [4] Y. Takeuchi, Y. Matsuzaki, K. Miyanishi, T. Sugiyama, and W. J. Munro, Quantum remote sensing with asymmetric information gain, *Phys. Rev. A* **99**, 022325 (2019).
 - [5] P. Yin, Y. Takeuchi, W.-H. Zhang, Z.-Q. Yin, Y. Matsuzaki, X.-X. Peng, X.-Y. Xu, J.-S. Xu, J.-S. Tang, Z.-Q. Zhou, G. Chen, C.-F. Li, and G.-C. Guo, Experimental demonstration of secure quantum remote sensing, *Phys. Rev. Appl.* **14**, 014065 (2020).
 - [6] N. Shettell, E. Kashefi, and D. Markham, Cryptographic approach to quantum metrology, *Phys. Rev. A* **105**, L010401 (2022).
 - [7] S. W. Moore and J. A. Dunningham, Secure quantum remote sensing without entanglement, *AVS Quantum Sci.* **5**, 014406 (2023).
 - [8] W. He, C. Huang, R. Guan, Y. Chen, Z. Zhang, and K. Wei, Experimental secure entanglement-free quantum remote sensing over 50 km of optical fiber, [arXiv:2412.18837](#).
 - [9] J. Ho, J. W. Webb, R. M. J. Brooks, F. Grasselli, E. Gauger, and A. Fedrizzi, Quantum-private distributed sensing, [arXiv:2410.00970](#).
 - [10] M. Hassani, S. Scheiner, M. G. A. Paris, and D. Markham, Privacy in networks of quantum sensors, *Phys. Rev. Lett.* **134**, 030802 (2025).
 - [11] L. Bugalho, M. Hassani, Y. Omar, and D. Markham, Private and robust states for distributed quantum sensing, *Quantum* **9**, 1596 (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, [arXiv:2505.02620](#).
 - [13] J. de Jong, S. Scheiner, N. R. Solomons, Z. Chaoui, D. Markham, and A. Pappa, Anonymous and private parameter estimation in networks of quantum sensors, *Phys. Rev. Appl.* **24**, 054053 (2025).
 - [14] U. Alushi and R. Di Candia, Privacy in distributed quantum sensing with Gaussian quantum networks, [arXiv:2509.22103](#).
 - [15] A. d. O. Junior, A. L. Andersen, B. L. Larsen, S. W. Moore, D. Markham, M. Takeoka, J. B. Brask, and U. L. Andersen, Privacy in continuous-variable distributed quantum sensing, [arXiv:2509.12338](#).

- [16] M. Bina, A. Mandarino, S. Olivares, and M. G. A. Paris, Drawbacks of the use of fidelity to assess quantum resources, *Phys. Rev. A* **89**, 012305 (2014).
- [17] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Theor. Comput. Sci.* **560**, 7 (2014).
- [18] A. K. Ekert, Quantum cryptography based on Bell's theorem, *Phys. Rev. Lett.* **67**, 661 (1991).
- [19] F. Grosshans and P. Grangier, Continuous variable quantum cryptography using coherent states, *Phys. Rev. Lett.* **88**, 057902 (2002).
- [20] S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, Asymptotic security of continuous-variable quantum key distribution with a discrete modulation, *Phys. Rev. X* **9**, 021059 (2019).
- [21] J. Lin, T. Upadhyaya, and N. Lütkenhaus, Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution, *Phys. Rev. X* **9**, 041064 (2019).
- [22] A. Denys, P. Brown, and A. Leverrier, Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation, *Quantum* **5**, 540 (2021).
- [23] F. Kanitschar, I. George, J. Lin, T. Upadhyaya, and N. Lütkenhaus, Finite-size security for discrete-modulated continuous-variable quantum key distribution protocols, *PRX Quantum* **4**, 040306 (2023).
- [24] M. Rosati, G. De Palma, A. Mari, and V. Giovannetti, Optimal quantum state discrimination via nested binary measurements, *Phys. Rev. A* **95**, 042307 (2017).
- [25] M. Bilkis, M. Rosati, R. M. Yepes, and J. Calsamiglia, Real-time calibration of coherent-state receivers: Learning by trial and error, *Phys. Rev. Res.* **2**, 033295 (2020).
- [26] M. Bilkis, M. Rosati, and J. Calsamiglia, Reinforcement-learning calibration of coherent-state receivers on variable-loss optical channels, in *2021 IEEE Information Theory Workshop* (IEEE, 2021), pp. 1–6.
- [27] M. Rosati and A. Solana, Joint-detection learning for optical communication at the quantum limit, *Opt. Quantum* **2**, 390 (2024).
- [28] M. Rosati and G. Cincotti, A Fourier machine for quantum optical communications, *J. Lightwave Technol.* **43**, 3770 (2025).
- [29] F. Kianvash and M. Rosati, Probabilistic pulse-position modulation for classical communication on quantum channels, *Phys. Rev. A* **112**, 032624 (2025).
- [30] M. N. Notarnicola, S. Olivares, E. Forestieri, E. Parente, L. Potì, and M. Secondini, Probabilistic amplitude shaping for continuous-variable quantum key distribution with discrete modulation over a wiretap channel, *IEEE Trans. Commun.* **72**, 375 (2024).
- [31] See Supplemental Material at <http://link.aps.org/supplemental/10.1103/rhgw-t21z> for detailed calculations of the MSE and the asymptotic limit.
- [32] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976), Vol. 84, p. 309.
- [33] J. E. Kolassa, *Series Approximation Methods in Statistics*, Lecture Notes in Statistics Vol. 88 (Springer, New York, 2006).
- [34] 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, *Phys. Rev. A* **87**, 012107 (2013).
- [35] To regenerate the data use the following https://figshare.com/articles/dataset/Private_Remote_Phase_Estimation_over_a_Lossy_Quantum_Channel/31141549?file=61299778.
- [36] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Experimental demonstration of long-distance continuous-variable quantum key distribution, *Nat. Photonics* **7**, 378 (2013).