Continuous Variable Measurement-Device-Independent Quantum Certification

B. L. Larsen,[1,*] A. A. E. Hajomer,[1] P. Abiuso,[2] S. Izumi,[1] T. Gehring,[1] J. S. Neergaard-Nielsen,[1] A. Acín,[3,4] and U. L. Andersen[1,†]

[1]*Center for Macroscopic Quantum States (bigQ) Department of Physics, Technical University of Denmark, Fysikvej 307, 2800 Kongens Lyngby, Denmark*

[2]*Institute for Quantum Optics and Quantum Information-IQOQI Vienna, Austrian Academy of Sciences, Boltzmanngasse 3, A-1090 Vienna, Austria*

[3]*ICFO-Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, Avinguda Carl Friedrich Gauss 3, 08860 Castelldefels (Barcelona), Spain*

[4]*ICREA-Institució Catalana de Recerca i Estudis Avançats, 08010 Barcelona, Spain*

(Received 1 April 2025; revised 16 October 2025; accepted 9 February 2026; published 30 March 2026)

Secure and reliable certification of quantum resources is a fundamental challenge in the advancement of next-generation quantum technologies, particularly as devices become more complex and integrated into practical applications, where parts of the system may be untrusted or inaccessible by users. Addressing this challenge requires certification methods that rely on minimal assumptions and limited trust while still faithfully and reliably verifying the quantum resources in question. For infinite-dimensional bosonic systems, existing certification methods rely on fully trusted and well-calibrated measurement systems, leaving significant security vulnerabilities open. In this work, we present the first experimental demonstration of measurement-device-independent (MDI) certification schemes for infinite-dimensional bosonic systems, where the certification process is conducted using entirely untrusted measurement devices and assuming only the trusted preparation of coherent states. Specifically, we implement schemes for the MDI certification of continuous-variable (CV) entanglement and the operation of an elementary optical CV quantum memory. We leverage techniques of Bayesian metrology and exploit the practicality and accessibility of Gaussian quantum optics to achieve secure and efficient certification. These results demonstrate the potential of the MDI framework to enhance trust in quantum technologies with applications in quantum communication and quantum computing.

DOI: 10.1103/g92b-2kwg

Subject Areas: Quantum Information

I. INTRODUCTION

How can a user with limited technological power certify the correct functioning of a complex uncharacterized quantum system? This is a crucial question in the development of quantum technologies, and various approaches have been explored to address it. A generic certification protocol begins by preparing the system in different possible states, $\{\psi^{(p)}\}$, then subjected to a set of possible channels $\{\Lambda^{(c)}\}$ and finally performing measurements on the system $\{M^{(m)}\}$. This process is repeated multiple times to gather sufficient data to estimate the statistics, $P_{\text{obs}} = \text{Tr}[\Lambda^{(c)}(\psi^{(p)})M^{(m)}]$ from which relevant properties can be certified [1,2]. Quantum state and quantum device tomography are well-known examples of this framework [see Fig. 1(a)] [3]. While these methods provide a robust and detailed form of certification, they are extremely resource intensive, requiring not only complete knowledge of the implemented measurements but also precise calibration and control of the experimental setup.

Device-independent (DI) protocols take a drastically different approach: they make no assumptions about the specific forms of states, channels, or measurements, treating them as "black boxes," with only their causal structure being given. For example, in a Bell test, if a Bell inequality violation is observed in the measurement statistics, the unknown state is confirmed to be entangled, regardless of the underlying hardware [4–6]. Likewise, a range of protocols has been established for certifying quantum devices using a DI approach [7,8] [see Fig. 1(b)]. However, DI protocols are experimentally challenging and often require balancing the necessary assumptions with technological feasibility.

*Contact author: blula@dtu.dk

†Contact author: ulun@dtu.dk

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

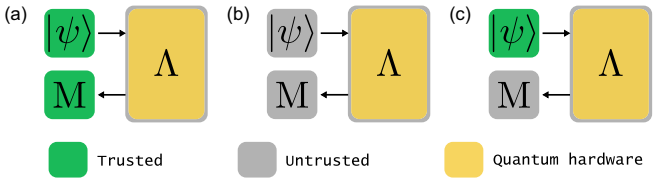


FIG. 1. Conceptual diagrams for the certification of quantum hardware represented by a channel Λ. (a) Certification relying on a trusted (green) source of probe states $|\psi\rangle$ and a trusted measurement apparatus M. (b) Certification in a fully device-independent scenario, where both the probe states and measurements are completely untrusted (gray). (c) Certification in the measurement-device-independent framework, using trusted probe states but untrusted measurement devices to validate the quantum device.

This motivates the formulation of semi-device-independent approaches, particularly the measurement-device-independent (MDI) framework, in which only a set of prepared states is fully trusted while other elements remain uncharacterized. Buscemi [9] and Branciard *et al.* [10] introduced MDI entanglement witnessing protocols, proving that entanglement of any finite-dimensional state can be detected in a Bell experiment with trusted quantum inputs—a result that has been experimentally verified [11,12] and used in applications [13–15]. Similar schemes have been developed and experimentally demonstrated for the MDI certification of quantum hardware [see Fig. 1(c)] [16–20].

While MDI protocols have also been applied to continuous-variable (CV) quantum key distribution [21], all existing demonstrations of MDI resource and hardware certification have been restricted to finite-dimensional systems. This is despite the fact that many critical quantum information protocols are based on CV systems [22]. These include CV quantum sensing [23,24], CV quantum key distribution [25], and CV quantum computing [26,27], each of which has exhibited quantum advantage.

In this article, we introduce an adversarial-metrology framework that can be used for MDI resource certification in CV systems and encompasses the recent theoretical proposals [28,29]. We present the first experimental MDI certification of CV entanglement, as well as MDI certification of an entanglement-preserving CV channel, akin to a CV transmission line or quantum memory. Specifically, leveraging the theoretical tools of quantum metrology, we implement CV witnesses for both state and channel certification that are independent of the specific operations of untrusted measurement devices, while relying only on the trusted preparation of coherent states.

II. MDI CERTIFICATION VIA QUANTUM METROLOGY

We start by considering the conventional strategy for certifying quantum resources, such as the detection of

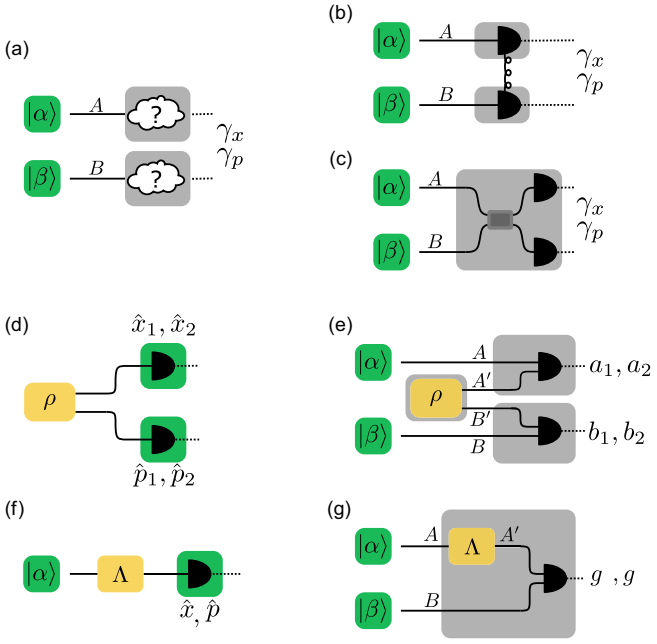


FIG. 2. Conceptual diagrams for MDI certification based on quantum metrology. (a) Alice and Bob prepare trusted coherent states, $\{|\alpha = \alpha_x + i\alpha_p\rangle\}$ and $\{|\beta = \beta_x + i\beta_p\rangle\}$, which are sent to Eve. Eve is asked to estimate the joint variables, $\gamma_x = \alpha_x - \beta_x$ and $\gamma_p = \alpha_p + \beta_p$. Strategies restricted to local measurements assisted by at most one-way communication limit her estimation precision to the bound given by the inequality in Eq. (2). However, by using either (b) an entangled state or (c) an entangling joint measurement strategy, this bound can be violated. (d)–(e) Certification of entanglement using trusted measurements (left) versus MDI certification with untrusted measurements but trusted coherent state sources (right). The violation of bound (2) implies that the shared state ρ must be entangled. (f)–(g) Certification of an entanglement-preserving channel, such as a quantum memory, using trusted measurements and sources (left) versus MDI certification with untrusted measurements and trusted coherent state sources (right). The violation of the bound in this case implies that the channel Λ is not a measure and prepare process (hence it is EP).

bipartite entanglement and the certification of an entanglement preserving quantum memory. In the former case, two parties, Alice and Bob, each receive one part of a bipartite state from an untrusted source, Eve. To verify the presence of CV entanglement, they perform well-calibrated quadrature measurement using homodyne or heterodyne detectors as illustrated in Fig. 2(d). The outcomes of these measurements are then evaluated using an entanglement witness such as the Duan-Simon inequality [30,31] for separable states: $\langle \mathrm{EW}\rangle = \langle \Delta^2(\hat{x}_1 - \hat{x}_2)\rangle + \langle \Delta^2(\hat{p}_1 + \hat{p}_2)\rangle \geq 2$. Here, using $\hbar = 1$, $\hat{x}_i$ and $\hat{p}_i$ represent the quadratures of the two modes, $i = 1, 2$ and $\langle \Delta^2 \hat{u}\rangle = \langle \hat{u}^2\rangle - \langle \hat{u}\rangle^2$. If the measurement results of Alice and Bob lead to a violation of this inequality, the presence of entanglement is confirmed. However, this method critically relies on the accurate calibration of the homodyne

detector systems. If the detectors are not properly calibrated, due to operational errors or external tampering, the computed variances may not accurately reflect the actual states. The measurement device must therefore be fully trusted.

Another example is the certification of a quantum memory [17], specifically corresponding to determining whether it preserves entanglement, which we dub an entanglement preserving (EP) channel (as opposed to entanglement breaking channels [32]). In other words, this involves verifying that the memory is able to store quantum states beyond simple classical storage, where states are measured, stored as classical bits, and then reconstructed [33]. Typically, this verification is performed by storing known quantum states, which are then released and subjected to quantum tomography to assess the fidelity of the memory process [as illustrated in Fig. 2(f)]. Also in this context, the reliability of the detectors is crucial; any malfunction or miscalibration can lead to inaccurate certification, thereby introducing security vulnerabilities.

MDI protocols avoid these issues by not relying on the faithful functioning of the measurement apparatus. In our case, we base the task of MDI entanglement or memory certification on a quantum metrology problem of estimating coherent states $|\alpha\rangle$ drawn from a Gaussian distribution $P(\alpha) = (\pi\sigma_x\sigma_p)^{-1}\exp\{-(\alpha_x^2/\sigma_x^2) - (\alpha_p^2/\sigma_p^2)\}$, where $\alpha \equiv \alpha_x + i\alpha_p$. The minimum uncertainty in estimating the quadrature $\alpha_x = \langle\hat{x}/\sqrt{2}\rangle$ and $\alpha_p = \langle\hat{p}/\sqrt{2}\rangle$ of a coherent state from a Gaussian distribution can be derived using the techniques of Bayesian metrology. The resulting optimal bound for the summed uncertainties, governed by the *a priori* information of the distribution, is given by (see Refs. [34,35] and the Appendix A)

$$\mathsf{Err}(\alpha_x) + \mathsf{Err}(\alpha_p) \geq \left(1 + \frac{1}{2\sigma_x^2} + \frac{1}{2\sigma_p^2}\right)^{-1} =: v(\sigma_x, \sigma_p), \tag{1}$$

where $\mathsf{Err}(\theta) := \langle(\hat{\theta} - \theta)^2\rangle$ represents the average square error of any estimator $\hat{\theta}$ of the parameter θ. It is known that the optimal measurement strategy, saturating the bound for a symmetric Gaussian distribution ($\sigma_x = \sigma_p$), is balanced heterodyne detection, where the $\hat{x}$ and $\hat{p}$ quadratures are simultaneously measured with equal uncertainty [36]. Notice however that the validity of (1) and the following (2) is not restricted to Gaussian measurements.

To derive a protocol for the MDI certification of quantum resources, we instead consider a variant of the previous metrology problem consisting in the estimation of the joint variables, $\gamma_x := \alpha_x - \beta_x, \gamma_p := \alpha_p + \beta_p$, from two independent coherent states, $|\alpha\rangle$ and $|\beta\rangle$, drawn from two Gaussian distributions. A straightforward approach is then to independently estimate the two coherent states with the minimal uncertainty found above, and subsequently estimate the joint variables through a linear combination of the measurement outcomes [see Fig. 2(a)]. This is indeed the optimal approach for estimating γ_x and γ_p when restricting the measurements to be local and assisted at most by one-way classical communication (see the Appendix A). Under such restrictions, it follows from Eq. (1) that the uncertainty in estimating the joint parameters will be lower bounded by the inequality

$$\mathsf{Err}(\gamma_x) + \mathsf{Err}(\gamma_p) \geq v(\sigma_{x,A}, \sigma_{p,A}) + v(\sigma_{x,B}, \sigma_{p,B}). \tag{2}$$

However, this bound can in general be violated, for example when using shared entanglement between the two detection sites [relaxing the classical correlation restriction, see Fig. 2(b)] or by performing nonlocal entangling measurements [thereby removing the locality restriction, see Fig. 2(c)]. These two types of entangling measurements are our primary tools for MDI resource certification: by broadcasting the outcomes of the entangling measurements, and subsequently violating Eq. (2), we may verify the presence of entanglement or certify the function of a quantum device (cf. Methods), using a framework akin (but not equivalent) to protocols for nonclassical teleportation [37,38], which leverage the same resources and are device dependent. The verification procedure is completely independent of the measurement devices, only requiring that the coherent states received by the detection systems are fully trusted [39]. Notice as well that for $\sigma_{x,B} = \sigma_{p,B} = 0$ the bound (2) recovers (1) as expected: in such case all the information about the variables $\gamma_{x,p}$ is encoded in $\alpha_{x,p}$ (up to constant β offset), and (2) can be thus saturated via local measurements. In order to verify quantum resources it is thus crucial that both parties generate a distribution of coherent states.

Having established the general MDI framework, we now specify it on the two certification tasks mentioned earlier: witnessing bipartite entanglement and certifying a quantum memory. The conceptual diagram of the corresponding entangling measurement schemes are illustrated in Figs. 2(e) and 2(g) and discussed in the following sections.

III. MDI CERTIFICATION OF CV ENTANGLEMENT

We return to the scenario where Alice and Bob seek to verify the presence of bipartite CV entanglement provided by an untrusted source, Eve. This verification can be achieved through a violation of the coherent state estimation bound in Eq. (2), which crucially does not depend on the trustworthiness of the detectors (also provided by Eve). The detection strategy shown in Fig. 2(e) allows for this. In this setup, Alice and Bob each prepare trusted coherent states of amplitudes $\alpha = \alpha_x + i\alpha_p$ and $\beta = \beta_x + i\beta_p$, sampled from Gaussian distributions with standard deviations σ. The two coherent states are then each measured

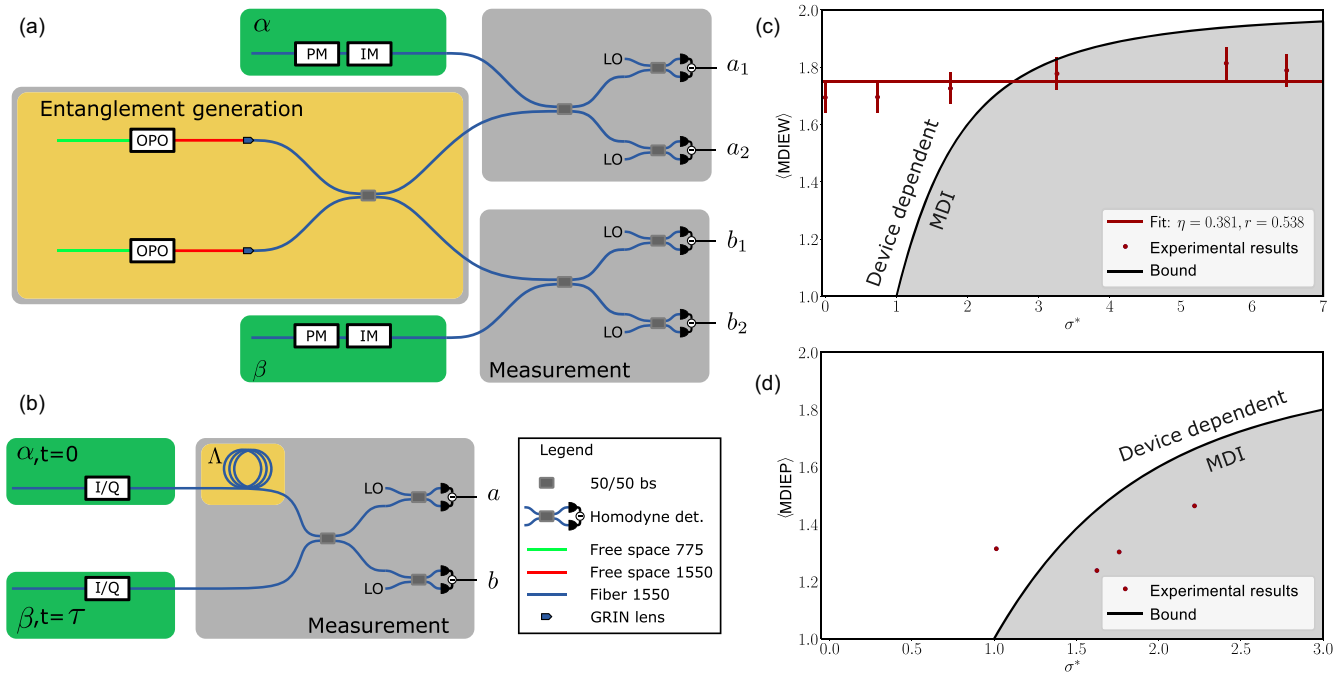


FIG. 3. MDI certification protocols of entanglement and a quantum memory. (a) Schematic of setup for entanglement witness. For the experiment we generate an entangled state in the yellow section and perform the measurement of $\{\hat{x}, \hat{p}\}$ in each measurement boxes. All beam splitters are 50/50. (b) Schematic of setup for memory verification. For the experiment we construct a memory for optical states with a 1 km long spool of fiber and perform the measurement of $\{\hat{x}, \hat{p}\}$ in the gray box. Experimental results demonstrating the MDI witness of (c) entangled TMSV state. The experimental data are fitted to the theoretical model developed in the main text and the Appendix B, Eq. (B6). The error bars correspond to 7000 frames of the experimental protocol, each frame consisting of 1000 coherent-state realizations in the MDIEW experiment. Panel (d) shows the results for the EP quantum memory. Ideally, the value of MDIEP witness should be independent of σ, although a weak dependence is observed here. We attribute this to phase noise in the fiber spool used as the memory, likely arising from uncontrolled environmental fluctuations in the laboratory. The error bars (smaller than plot markers) indicate the 95% confidence intervals. Red dots are the experimental values of the witness, while the solid black line indicates the theoretical upper bound of the witness. The shaded gray area delineates the MDI certification region for the protocols. The value of the witness in (c) and (d) is below 2 for all values of σ^* thus violating the device dependent Simon-Duan bound and memory certification bound.

locally, together with one mode of the bipartite entangled state under test. These two local measurements are each realized using two heterodyne detectors, effectively implementing a CV Bell state measurement. Notice here that this causal structure [see Fig. 2(e)] is guaranteed if Alice and Bob operate locally the untrusted devices provided by Eve. Four quadrature measurements are therefore obtained, coined $\{a_1, a_2, b_1, b_2\}$, and used to estimate $\gamma_{x,p}$. That is, Alice and Bob compute the left-hand side of the witness inequality in Eq. (2), defined as $\langle \mathrm{MDIEW} \rangle = \langle (a_1 - b_1 - (\alpha_x - \beta_x))^2 \rangle + \langle [a_2 + b_2 - (\alpha_p + \beta_p)]^2 \rangle \simeq \mathsf{Err}(\gamma_x) + \mathsf{Err}(\gamma_p)$, that is, taking $a_1 - b_1$ and $a_2 + b_2$ as the estimators of γ_x and γ_p, respectively.

Entanglement is then confirmed if $\langle \mathrm{MDIEW} \rangle < 2\nu(\sigma, \sigma) = 2\sigma^2/(1+\sigma^2)$ assuming symmetric distributions $\sigma = \sigma_{x,A} = \sigma_{p,A} = \sigma_{x,B} = \sigma_{p,B}$ for simplicity.

To explore the parameter space for which entanglement can be detected, we compute the expected value of the left-hand side of the inequality in Eq. (2) for ρ being a two-mode squeezed vacuum state (TMSV) characterized by a squeezing parameter r and subject to losses of $1-\eta$. The resulting value is $\langle \mathrm{MDIEW} \rangle = 2 + \eta(e^{-2r} - 1)$ (see the Appendix B, or [28]). Thus, the condition for MDI entanglement detection is given by $\eta(1 - e^{-2r}) > 2/(1+\sigma^2)$, assuming symmetric and identical coherent state distributions for both sources. It is evident that for large coherent state distributions ($\sigma \gg 1$), MDI detection of entanglement is feasible regardless of the degree of squeezing. In contrast, for narrow distributions, more stringent requirements are imposed on both the transmission coefficient η, and the squeezing parameter, r.

To demonstrate the MDI entanglement verification protocol (see Fig. 3), we generate bipartite entanglement in the form of a TMSV, achieved by interfering two single-mode squeezed states on a fiber beam splitter. The resulting entangled modes are then sent to two separate measurement stations, where they are jointly measured with trusted coherent states using heterodyne detection systems. Each system comprises a symmetric beam splitter and two high

efficiency balanced homodyne detectors, set to detect the conjugate quadratures, x and p. The coherent states, used as trusted inputs, are generated at a sideband frequency of 3.1 MHz via an intensity and phase modulator (IM and PM) controlled by an arbitrary waveform generator. The sideband frequency was chosen to operate within the region of maximal squeezing of the OPOs, corresponding to their 8.35 MHz bandwidth.

The MDI protocol proceeds as follows: First, full calibration of the input coherent state distributions is performed as a preliminary step. Following this, in each round, two trusted random coherent states are generated and injected, along with their respective TMSV entangled modes into the untrusted detection systems [see Fig. 3(a)]. The measurement outcomes are then recorded for subsequent analysis. The four outcomes, associated with the homodyne detectors, are then combined to form the joint variables $\{a_1 - b_1, a_2 + b_2\}$ used as estimators of $\{\gamma_x, \gamma_p\}$. We repeat the protocol with 1000 independently generated pairs of coherent states $\{\alpha, \beta\}$ drawn from the Gaussian distributions of widths $\sigma_{x,A}$, $\sigma_{p,A}$, $\sigma_{x,B}$ and $\sigma_{p,B}$. From these measurements, we compute the errors of the joint variables and sum the results to evaluate the left-hand side of Eq. (2), checking for any potential violations. To explore the effect of the input distributions, we vary the widths and, for each setting, perform measurements using 7000 identical frames, where each frame consists of 1000 coherent states in order to estimate the statistical variance of the error of the measured witness.

The summed errors obtained for six different distribution widths are shown in Fig. 3(c), and compared against the threshold required for MDI verification of entanglement Eq. (2). These results clearly demonstrate the successful observation of entanglement in a manner compliant with the MDI framework. Notice that here (and in the following memory certification Sec. IV) we introduce in the figures an effective average variance, σ^*, defined such that $2v(\sigma^*, \sigma^*) \equiv v(\sigma_{x,A}, \sigma_{p,A}) + v(\sigma_{x,B}, \sigma_{p,B})$, in order to account for the slight asymmetry in the widths.

It is important emphasizing that the metrological MDI witness Eq. (2) is fully adversarial. It means it accounts for the possibility that Eve, over time, could estimate the quantum input distribution (parametrized by σ^* in our case) and consequently optimize her estimation strategy. However, the implemented experimental protocol is independent of the input distribution and is designed to achieve the same average error for any given value of $\gamma_{x,p}$. This shows that, for sufficiently large σ^*, the presence of entanglement can be reliably detected without requiring Eve to perform the (*a priori* nontrivial) estimation of the input distribution. In our theoretical analysis, we assumed that Alice and Bob could increase σ^* at no added cost. In practice, however, the phase noise associated with high-amplitude coherent states hinders such assumption. Nevertheless, it is plausible that with knowledge of σ^*, the estimation protocol could be optimized to detect entanglement even at low values of σ^*. For instance, one such optimization involves postprocessing the outputs of the homodyne measurements via a simple rescaling of the quadrature data: $\{a_1, a_2, b_1, b_2\} \to \{\epsilon a_1, \epsilon a_2, \epsilon b_1, \epsilon b_2\}$. In the Appendix B we show that such a rescaling extends the range of TMSV states for which entanglement is witnessed. The error observed by Alice and Bob with rescaling is

$$\begin{aligned}\langle \mathcal{E} \rangle(\epsilon, \sigma^*, r) &= \mathsf{Err}(\gamma_x) + \mathsf{Err}(\gamma_p) \\ &= \epsilon^2 \mathrm{e}^{-2r} + \epsilon^2 + 2(\epsilon - 1)^2 \sigma^{*2}, \end{aligned} \tag{3}$$

which can violate Eq. (2) for $r > 0$ and $\sigma^* > 0$. Importantly, any such optimization procedure can only *improve* MDI entanglement detection, but cannot produce *false* positives. That is, in the absence of entanglement ($r = 0$), Eq. (2) remains valid *regardless* of the rescaling applied.

In contrast, device-dependent entanglement witnesses may yield false positives under similar conditions: For example, applying the Simon-Duan criterion to a rescaled system results in $\langle \mathrm{EW} \rangle(\epsilon) = \langle \Delta^2(\epsilon \hat{x}_1 - \epsilon \hat{x}_2) \rangle + \langle \Delta^2(\epsilon \hat{p}_1 + \epsilon \hat{x}_2) \rangle = 2\epsilon^2$. Here a violation of the witness is observed for $\epsilon < 1$, even in the absence of entanglement.

We showcase this comparison in Fig. 4 where we plot $\langle \mathcal{E} \rangle(\epsilon, \sigma^*, r) - 2v(\sigma^*, \sigma^*)$, for which a value below 0 is a violation of the MDIEW witness, as a function of the rescaling ϵ and σ^* with existing squeezing $r = 0.2$. We show how the rescaling can lead to violation of the MDIEW bound with lower values of σ^*.

One should note that while being able to witness the entanglement of all Gaussian entangled states [28], our framework can be used to witness non-Gaussian states as well, e.g., whenever they violate the Simon-Duan bound, by repeating the same construction. As an example, the split photon subtracted single-mode squeezed vacuum state $\hat{U}_{12}^{BS} \hat{a}_1 \hat{S}_1(r) |0, 0\rangle$ is entangled for all values of $r > 0$ and violates the Simon-Duan bound for values of $r \gtrapprox 0.55$ [40]. Including such state, proposals for an experimentally feasible (though device-dependent) entanglement witnessing protocol for non-Gaussian CV states have recently been put forward in [40].

Finally, we comment on the effect of finite-size sampling statistics on the security of our protocol. Finite averaging prevents a perfect estimation of the errors in Eq. (2) perfectly, and statistical fluctuations may, in principle, allow a (lucky) adversary to spuriously violate the MDIEW even in the absence of entanglement. Such statistical fluctuations are increasingly suppressed as the number of random experimental repetitions grows. In the Appendix B, we apply Hoeffding's inequality to derive an upper bound on the probability of such finite-sample violations. For our largest value of σ^*, this bound is found to be 4.2%. This implies that a malicious Eve, in the absence of entanglement, would have less than 5%

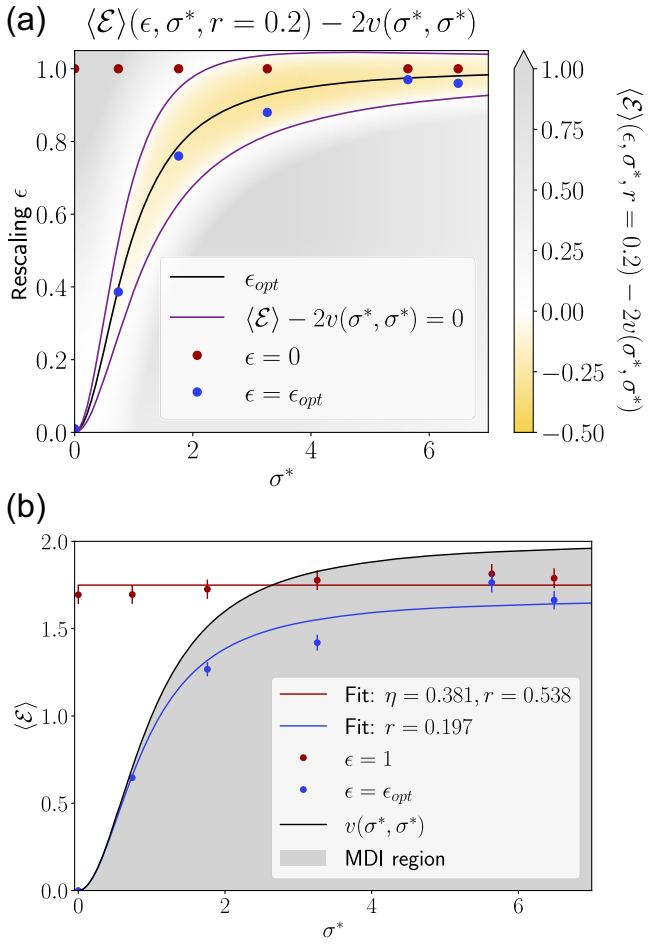


FIG. 4. (a) The value of $\langle\mathcal{E}\rangle(\epsilon,\sigma^*,r)-2v(\sigma^*,\sigma^*)$. A value below 0 implies MDI entanglement witness. The black curve is the optimal ϵ for the ideal case (no loss and phase noise). The white curves are $\langle\mathcal{E}\rangle(\epsilon,\sigma^*,r)=2v(\sigma^*,\sigma^*)$ between which the MDI entanglement witness can be performed. Red dots are experimental values without rescaling $\epsilon=1$ and blue dots are with the optimal rescaling $\epsilon=\epsilon_{\mathrm{opt}}$. (b) is a reproduction of Fig. 3(c) but with optimized ϵ. The experimental data is fitted to the model developed in the Appendix B Eq. (B6) in ($\epsilon=1$) and Eq. (B12) (ϵ_{opt}).

probability of achieving an MDIEW score equal to or better than the experimental average when performing the protocol with 1000 random coherent-state inputs under individual attacks. We further note that the same analysis yields a vanishingly small probability in the case of the memory witness discussed in Sec. IV, due to the substantially larger sample size used there.

IV. MDI CERTIFICATION OF A CV QUANTUM MEMORY

Having successfully demonstrated MDI entanglement verification, we now employ the MDI framework to certify the operation of a quantum memory, ideally behaving as an identity channel ($\Lambda\approx\mathbb{I}$), in control of an untrusted party, Eve [see Fig. 2(g)]. In this protocol the user, Alice, prepares trusted coherent states, $|\alpha\rangle$ and $|\beta\rangle$, sampled independently from Gaussian distributions. Unlike in the entanglement verification protocol, the states are prepared asynchronously: $|\alpha\rangle$ is stored in the quantum memory, while $|\beta\rangle$ is prepared later. After a storage period, the state $|\alpha\rangle$ is released from the memory and then jointly measured with $|\beta\rangle$ using a CV Bell state measurement. Eve performs the joint measurement and obtains the quadrature outcomes $\{g_x,g_p\}$. From these outcomes, we construct the witness: $\langle\mathrm{MDIEP}\rangle=\langle(g_x-\gamma_x)^2\rangle+\langle(g_p-\gamma_p)^2\rangle\simeq\mathsf{Err}(\gamma_x)+\mathsf{Err}(\gamma_p)$. The entanglement-preserving nature of the quantum memory is verified if $\langle\mathrm{MDIEP}\rangle<2v(\sigma^*,\sigma^*)$. In contrast to the previous protocol, where the violation indicated the presence of entanglement in the shared state, here the violation arises due to the possibility of Eve performing (quantum) nonlocal measurement only using an EP memory: in fact, an entanglement-breaking memory acting on the first input would make the overall measurement on $|\alpha\rangle$ and $|\beta\rangle$ effectively local (see details in Methods), thus obeying the bound (2).

We now analyze the parameter space in which the EP nature of a simple quantum memory can be certified using the MDI framework. To do this, we compute the expected value of the left-hand side of Eq. (2) for our system, taking into account both memory loss characterized by the transmission efficiency η and the presence of excess noise ξ. Under these noise conditions, entanglement preservation is achieved when the following inequality holds: $\langle\mathrm{MDIEP}\rangle=[1/(2\eta)](2+\xi+\eta\xi)\geq 2v(\sigma^*,\sigma^*)$, where we assume that the coherent state distributions are symmetric and identical (see the Appendix B). The inequality is illustrated in Fig. 3(d), showing the regions of the parameter space where the MDI entanglement-preserving properties of the memory can be detected. The results indicate that only specific combinations of η, ξ, and σ, allow for the successful certification of EP features. For instance, in the regime of broad coherent state distributions ($\sigma\gg 0$) and no excess noise ($\xi=0$), MDI entanglement-preserving certification is feasible even with high memory loss. However, for narrow distributions and nonzero excess noise ($\xi\neq 0$), stricter requirements are imposed on the transmission efficiency η for the detection of entanglement preservation.

We experimentally implement MDI memory certification using the setup shown in Fig. 3(b). The trusted coherent states, $|\alpha\rangle$ and $|\beta\rangle$, are prepared in a 10 MHz wide baseband using quadrature modulation. The quantum memory is implemented using a 1 km fiber spool, providing a storage time of 4.9 μs and a transmission efficiency of $\eta\approx 0.8$ and negligible excess noise, $\xi\approx 0$. The CV Bell state measurement is performed by overlapping the two states on a polarization beam splitter, followed by a 90° polarization-based hybrid to detect the orthogonal quadrature. Additional details on the system implementation are provided in the Methods section and the Appendix B.

Using the collected measurements, we calculate the errors of the joint variables following the procedure outlined in the entanglement witness protocol. We then evaluate $\langle \mathrm{MDIEP} \rangle$ to assess whether the obtained values violate the bound specified in Eq. (2). To explore the impact of the input states, we systematically vary the widths of the coherent state distributions and perform measurements for each setting, with 2×10^6 coherent states for each value of σ^*. The results for four different distribution widths are presented in Fig. 3(d). These results clearly show violations of the MDI certification threshold for the three largest distribution widths, thereby confirming the successful and robust operation of the quantum memory. In fact, due to the high number of measurements per witness (2×10^6) and the exponential scaling of Hoeffding's inequality, the probability of false positives due to finite-size sampling is, in the absence of quantum memory, very close to zero (less than 10^{-100}). See the Appendix A for details.

V. CONCLUSION

In this work we have reported the successful certification of CV Gaussian entangled states and quantum memories within the MDI framework. Our approach relies solely on the trusted preparation of single-mode coherent states of light, arguably one of the simplest sets of states to prepare in the lab. This minimal assumption is a significant advantage, as it allows the rest of the hardware to remain fully uncharacterized (i.e., it can perform any operation allowed by quantum mechanics), offering strong security guarantees even when parts of the hardware are under the control of an untrusted party. Gaussian quantum optics, which has reached the level of a mature technology and is available in most experimental facilities, cannot be used for fully device-independent protocols. However, as demonstrated in this work, introducing minimal trust through the MDI scenario fundamentally changes the perspective.

This demonstration of MDI resource and device certification represents an important step towards further applications of MDI protocols in the realm of CV quantum information. As quantum technologies continue to advance, we anticipate scenarios where users with limited technological capabilities will need to interact with large quantum service providers. In such contexts, MDI schemes like those demonstrated here could serve as essential building blocks for secure protocols and reliable certification, offering strong security guarantees even when the user must rely on external, potentially untrusted hardware.

VI. METHODS

A. Units and normalization for continuous-variable quantum systems

We use standard units for bosonic operators and quadratures, defined as

$$\hat{x} = \frac{\hat{a} + \hat{a}^\dagger}{\sqrt{2}}, \qquad \hat{p} = \frac{\hat{a} - \hat{a}^\dagger}{\sqrt{2}i}, \tag{4}$$

where $\hat{a}$, $\hat{a}^\dagger$ are the canonical annihilation and creation operators, respectively. It follows that $[\hat{x}, \hat{p}] = i$, and the uncertainty principle reads $\mathrm{Var}[\hat{p}]\mathrm{Var}[\hat{x}] \geq \frac{1}{4}$. Coherent states are defined as

$$|\alpha\rangle = e^{i\sqrt{2}\alpha_p \hat{x} - i\sqrt{2}\alpha_x \hat{p}}|0\rangle = e^{\alpha\hat{a}^\dagger - \alpha^* \hat{a}}|0\rangle, \tag{5}$$

where $\alpha = \alpha_x + i\alpha_p$. In these units, the variances of the quadratures for a coherent state (including the vacuum state) are equal to $\frac{1}{2}$, and the mean values satisfy $\langle \alpha|\hat{x}|\alpha\rangle = \sqrt{2}\alpha_x$ and $\langle \alpha|\hat{p}|\alpha\rangle = \sqrt{2}\alpha_p$.

B. Witnessing of quantum resources via the limits of 1-LOCC measurements

Our main tool for MDI certification is the inequality (2), which is valid (see the Appendix A) for 1-LOCC measurements (local operations and one-way classical communication). A measurement on two systems A and B is 1-LOCC if it can be expressed as of the form

$$\mathcal{M}_{AB}^{(\text{1-LOCC})a,b} = \sum_i P(i) \mathcal{M}_A^{(i)a} \otimes \mathcal{M}_B^{(i)b|a}, \tag{6}$$

where $\mathcal{M}_A^{(i)a}$ and $\mathcal{M}_B^{(i)b|a}$ are general local quantum measurements satisfying $\sum_a \mathcal{M}_A^{(i)a} = \mathbb{I}$ and $\sum_b \mathcal{M}_B^{(i)b|a} = \mathbb{I}$. $P(i)$ represents a random variable shared between the systems, and $\mathcal{M}_B^{(i)b|a}$ depends on A's outcome a. This decomposition captures local measurements assisted by the possibility of one-way communication from A to B.

1. MDI entanglement witnessing

In the Bell-like experiment presented in Fig. 2(e), coherent states $|\alpha\rangle$ and $|\beta\rangle$ are sent to causally separated [41] measurement stations A and B, which may share a bipartite state $\rho_{A'B'}$. Given the locality of the two measurement stations A and B, and making no other assumptions on the experimental devices other than this causal structure, the general form of their statistical output takes the form

$$\begin{aligned} &P(a, b||\alpha\rangle, |\beta\rangle) \\ &= \mathrm{Tr}\Big[(|\alpha\rangle\langle\alpha|_A \otimes \rho_{A'B'} \otimes |\beta\rangle\langle\beta|_B) M_{AA'}^a \otimes M_{BB'}^b\Big] \\ &= \mathrm{Tr}\Big[(|\alpha\rangle\langle\alpha|_A \otimes |\beta\rangle\langle\beta|_B) \mathcal{M}_{AB}^{a,b}\Big], \end{aligned} \tag{7}$$

where $\mathcal{M}_{AB}$ is an effective measurement acting on the input coherent states and producing outputs $\{a, b\}$. If the shared state $\rho_{A'B'}$ is separable, i.e., $\rho_{A'B'} = \sum_i p_i \rho_{A'}^{(i)} \otimes \rho_{B'}^{(i)}$, the induced measurement becomes separable:

$$\mathcal{M}_{AB}^{a,b} \coloneqq \mathrm{Tr}_{A'B'}\left[\rho_{A'B'} M_{AA'}^{a} \otimes M_{BB'}^{b}\right] \overset{\mathrm{SEP}}{=} \sum_i p_i \mathcal{M}_A^{(i)a} \otimes \mathcal{M}_B^{(i)b}. \quad (8)$$

Such measurements are of the 1-LOCC form Eq. (6). Thus, violation of the inequality (2) serves as an MDI witness of entanglement.

Our experimental setup (Sec. III) uses this framework to certify the entanglement of a TMSV state. Moreover, the related generalized MDI bound (2) introduced in [28], extends the Simon-Duan criterion [30,31] to detect any entangled Gaussian state.

2. MDI quantum memory certification

The protocol for MDI quantum memory is schematically depicted in Fig. 2(g). There, a random coherent state $|\alpha\rangle$ is sent to the adversary station at time $t = 0$, while a second state $|\beta\rangle$ is sent after a time delay $t = \tau$, forcing the use of the memory for at least τ. Under this causal structure, the output statistics are given by

$$P(b||\alpha\rangle, |\beta\rangle) = \mathrm{Tr}[M_{AB}^{b}(\Lambda \otimes \mathbb{I})[|\alpha\rangle\langle\alpha|_A \otimes |\beta\rangle\langle\beta|_B]_{A'B}] \quad (9)$$

$$\overset{\mathrm{EB}}{=} \sum_a \mathrm{Tr}\left[M_{A'B}^{b}(\rho_{A'}^{(a)} \otimes |\beta\rangle\langle\beta|_B)\right]\mathrm{Tr}[M_A^a|\alpha\rangle\langle\alpha|_A], \quad (10)$$

where $M_{A'B}^{b}$ represents the measurement operator, and Λ is the channel applied by the memory. The last equality (10) holds if the channel Λ from A to A' is entanglement breaking (EB). EB channels can always be represented in the measure-and-prepare form: $\Lambda[\rho_A]_{A'} \overset{\mathrm{EB}}{=} \sum_a \rho_{A'}^{(a)} \mathrm{Tr}[M_A \rho_A]$ [32]. In such case, without loss of generality, the virtual output a can be copied and transmitted to the output port, resulting in an effective statistics (a, b) obtained via the measurement

$$\mathcal{M}_{AB}^{a,b} \overset{\mathrm{EB}}{=} M_A^a \otimes \mathrm{Tr}_{A'}\left[M_{A'B}^{b}\rho_{A'}^{(a)}\right]. \quad (11)$$

This measurement process adheres to the 1-LOCC form described in Eq. (6). Therefore, any violation of the inequality Eq. (2) confirms that the memory is not entanglement-breaking, certifying its entanglement-preserving properties.

C. Entanglement witness

1. Entangled resource

The entangled TMSV state is generated by interfering two single-mode squeezed states produced by two identical optical parametric oscillators (OPO). Each OPO uses a bow-tie cavity configuration with a periodically poled potassium titanyl phosphate (PPKTP) crystal as the nonlinear medium. Each OPO is injected with a 1550 nm probe beam derived from a laser source (NKT Photonics X-15), while the pump at 775 nm, required for the parametric process, is generated through second harmonic generation in another bow-tie cavity. To ensure stable operation, each cavity is locked using a dedicated locking beam at 1550 nm, which counterpropagates within the bow-tie cavity. The probe beam incorporates a piezomounted mirror, modulated with signals at $S_{\mathrm{OPO1}} = 17$ and $S_{\mathrm{OPO2}} = 26$ kHz, respectively. For locking the relative phase of the OPOs, 1% of the output light from the cavity is tapped off and demodulated to produce an error signal. This feedback signal allows the system to lock at 0 (π) relative phase between probe and pump, ensuring deamplification (amplification) of the parametric process. This results in one mode being squeezed in amplitude and the other in phase.

Feedback control for locking systems is managed using the PYRPL software [42] running on RedPitaya FPGA boards. These boards feature integrated fast ADCs and DACs, enabling precise real-time control. The cavity locks are implemented using the Pound-Drever-Hall (PDH) technique [43].

The single-mode squeezed states are coupled into optical fibers and subsequently interfered on a 50/50 fiber coupler with a controlled relative phase difference of 0. This interference generates the TMSV state. To maintain the correct phase between the two single-mode squeezed states, a small fraction (1%) of the output light from one arm of the fiber coupler is tapped using a 99/1 beam splitter. The relative phase is then measured, and a fiber stretcher is used to adjust the phase of one of the single-mode squeezed states accordingly. The phase locking system utilizes the modulation signal S_{OPO2}, which is also used for controlling the parametric gain of OPO2.

2. Homodyne detection and data collection

Quadrature measurements for both Alice and Bob are performed using four custom-built balanced homodyne detectors (HD), which measure the $\hat{x}$ and $\hat{p}$ quadratures. The phase between the local oscillator (LO) and the signal is locked using a fiber stretcher in the LO path. Locking ensures precise alignment with the $\hat{x}$ and $\hat{p}$ quadratures and is achieved through the sidebands S_x and S_p generated alongside the coherent states.

The HD employs high-efficiency photodiodes with 99% quantum efficiency (according to spec sheet from manufacturer). Light from the fiber is coupled onto the photo diodes using antireflection coated graded-index (GRIN) lenses. To address the slight imbalances in the 50/50 beam splitter (BS), caused by variations in its splitting ratio and polarization sensitivity, bending losses are introduced in one arm of the fiber arms. These losses are controlled using a small, adjustable 3D-printed component that bends the fiber, with fine-tuning performed via a screw mechanism. Additionally, a polarization controller is placed in the LO path to optimize the visibility between the LO and the signal, ensuring high-quality interference.

The RedPitaya FPGA boards play a central role in the system. They generate intensity and phase modulation (IM and PM) signals and perform demodulation of the ac signals, measuring the locking signals S_x and S_p sidebands to maintain stable operation.

The data from the homodyne detectors is collected using the RedPitaya boards. Demodulation of the ac signals is performed directly within the boards. To prevent interference and beating between the locking and data collection modulation signals, RedPitayas are synchronized through their clocks. The boards are connected to a PC via an ethernet connection, which is used to store the measurement traces and generate the coherent state alphabets. To minimize laser noise during the measurement, a lock-measure scheme is implemented. In this scheme the lock-measure signal acts as a trigger, with the first half of the measurement trace taken during the locking phase and the second half during the measurement phase. To eliminate potential leakage in the acousto-optic modulator (AOM) during the transition, only the last 7700 data points of each measurement trace are used for analysis. A function generator is used to generate a square signal, used for both lock-measure and trigger of detection in the RedPiatayas. The square signal is operating at 10 Hz allowing sufficient time for data saving on the PC. Each individual measurement trace contains 2^{14} data points.

D. Memory certification

The user (Alice) generated an ensemble of coherent states by modulating a 1550 nm continuous wave laser using in-phase and quadrature modulators driven by digital-to-analog converters (DACs). The two driving waveforms were generated digitally using the digital signal processing (DSP) chain, as described in [44]. This DSP module includes a quantum random generator (QRNG) based on vacuum fluctuations [44], which provides the complex amplitude of the coherent states at a repetition rate of 10 MHz. These quantum symbols were then upsampled to the DACs sampling rate of 1 GSample/s and pulse-shaped using a root-raised cosine filter with a roll-off factor of 0.2. A 16 MHz pilot tone was added to the signal for phase compensation. Automatic bias controllers (ABC) were employed to stabilize the bias voltages of the IQ modulators. To fine-tune the size of the generated alphabet, variable optical attenuators (VOAs) were used after the IQ modulators. Subsequently, one of the generated states was stored in the quantum memory, which was made of 1 km standard single mode fiber, with a storage time of 4.9 μS and efficiency of ≈80%. To compensate for polarization rotation in the memory, a manual polarization controller was used before the memory. The other state was connected to the measurement device through a fiber patch cord. A polarization 90° hybrid relay was utilized to perform the CV Bell measurement [44]. Further details on the operational principles of this relay can be found in Ref. [44].

The signals were then detected and digitized using balanced detectors with a shot-noise limited bandwidth of 13 MHz and a 1 GSample/s analog-to-digital converter (ADC). Finally, the quadrature values were recovered using the DSP routine [44], which includes phase compensation using the pilot tone and quadrature remapping, time synchronization, matched filtering, and downsampling. A figure of the experimental setup can be seen in the Appendix B.

ACKNOWLEDGMENTS

B. L. L., A. A. E. H., S. I., T. G., J. S. N-N., and U. L. A. were supported by the Danish National Research Foundation (bigQ, DNRF0142), EU Horizon Europe (QSNP, Grant No. 101114043) and the Innovation Foundation Denmark (CyberQ). In addition A. A. E. H. and T. G. were supported by Carlsberg Foundation (Project No. CF21-046). P. A. was supported by the QuantERA II programme, that has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 101017733, and from the Austrian Science Fund (FWF), Project No. ESP2889224. A. A. was supported by the Government of Spain (Severo Ochoa CEX2019-000910-S, European Union NextGenerationEU PRTR-C17.I1 and FUNQIP), Fundació Cellex, Fundació Mir-Puig, Generalitat de Catalunya (CERCA program), the European Union (QSNP, 101114043 and Quantera project Veriqtas), the ERC AdG CERQUTE, and the AXA Chair in Quantum Information Science.

DATA AVAILABILITY

The data are not publicly available. The data are available from the authors upon reasonable request.

APPENDIX A: MAIN METROLOGICAL BOUNDS

1. Main bounds

Here, we derive the Bayesian Cramér-Rao bound presented in Eq. (1) of the main text. Specifically, we show that for a Gaussian prior distribution

$$P(\alpha;\sigma_x,\sigma_p)=\frac{e^{-\alpha_x^2/\sigma_x^2-\alpha_p^2/\sigma_p^2}}{\pi\sigma_x\sigma_p}, \tag{A1}$$

the minimum average combined error for the simultaneous estimation of α_x and α_p encoded in the coherent state $|\alpha_x+i\alpha_p\rangle$, satisfies

$$\mathsf{Err}(\hat{\alpha}_x)+\mathsf{Err}(\hat{\alpha}_p)\geq\left(1+\frac{1}{2\sigma_x^2}+\frac{1}{2\sigma_p^2}\right)^{-1}, \tag{A2}$$

where $\mathsf{Err}(\theta):=\langle(\hat{\theta}-\theta)^2\rangle$ represents the average square error of any estimator $\hat{\theta}$ of the parameter θ. In the special

case where $\sigma_x = \sigma_p$, the bound simplifies to $\mathsf{Err}(\hat{\alpha}_x) + \mathsf{Err}(\hat{\alpha}_p) \geq [\sigma^2/(1+\sigma^2)]$. This specific result is known and has been previously reported in the literature (see, e.g., [34–36,45,46]). Here, we generalize it to the case where $\sigma_x \neq \sigma_p$, following the approach of [34].

Proof of Eq. (A2) [Eq. (1) in main text]. We start by defining the complex estimator observable

$$\hat{\alpha} \coloneqq \hat{\alpha}_x + i\hat{\alpha}_p. \tag{A3}$$

The goal is to find a lower bound on the average squared error:

$$\langle|\hat{\alpha}-\alpha|^2\rangle = \int \mathrm{d}^2\alpha P(\alpha)\mathrm{Tr}[(\hat{\alpha}-\alpha)(\hat{\alpha}^\dagger-\alpha^*)|\alpha\rangle\langle\alpha|]. \tag{A4}$$

Consider the expression

$$B(\alpha) \coloneqq P(\alpha)\mathrm{Tr}[(\hat{\alpha}-\alpha)|\alpha\rangle\langle\alpha|]. \tag{A5}$$

Here, $B(\alpha)$ represents the average bias of the estimator $\hat{\alpha}$ weighted by the prior distribution $P(\alpha)$, which is Gaussian in our case. Assuming the bias grows at most polynomially in α, we have

$$\int \mathrm{d}^2\alpha \frac{\partial B(\alpha)}{\partial\alpha} = 0, \tag{A6}$$

which translates to

$$\int \mathrm{d}^2\alpha P(\alpha)\frac{\partial \ln P(\alpha)}{\partial\alpha}\mathrm{Tr}[(\hat{\alpha}-\alpha)|\alpha\rangle\langle\alpha|] + P(\alpha)\mathrm{Tr}[(\hat{\alpha}-\alpha)|\alpha\rangle\langle\alpha|L_\alpha^\dagger] = 1, \tag{A7}$$

where L_α is the *right logarithmic derivative* (RLD) [34,36], defined by the equation $\partial_\alpha\rho(\alpha) = \rho(\alpha)L_\alpha^\dagger$. We thus have

$$1 = \int \mathrm{d}^2\alpha P(\alpha)\mathrm{Tr}\left[(\hat{\alpha}-\alpha)\left(\frac{\partial \ln P(\alpha)}{\partial\alpha} + L_\alpha^\dagger\right)\right]. \tag{A8}$$

Using the Cauchy-Schwarz inequality for the scalar product $\langle\!\langle O_1, O_2\rangle\!\rangle \coloneqq \int \mathrm{d}^2\alpha P(\alpha)\mathrm{Tr}\{|\alpha\rangle\langle\alpha|O_1^\dagger(\alpha)O_2(\alpha)\}$, we obtain

$$1 \leq \mathcal{F}\int \mathrm{d}^2\alpha P(\alpha)\mathrm{Tr}[(\hat{\alpha}-\alpha)(\hat{\alpha}^\dagger-\alpha^*)|\alpha\rangle\langle\alpha|], \tag{A9}$$

or, equivalently, $\langle|\hat{\alpha}-\alpha|^2\rangle \geq \mathcal{F}^{-1}$, where $\mathcal{F}$ is defined as

$$\mathcal{F} \coloneqq \int \mathrm{d}^2\alpha P(\alpha)\left[|\alpha\rangle\langle\alpha|\left(\frac{\partial \ln P(\alpha)^*}{\partial\alpha} + L_\alpha\right)\left(\frac{\partial \ln P(\alpha)}{\partial\alpha} + L_\alpha^\dagger\right)\right]. \tag{A10}$$

Evaluating $\mathcal{F}$, we find that it separates into two terms:

$$\mathcal{F} = \int \mathrm{d}^2\alpha P(\alpha)\left|\frac{\partial \ln P(\alpha)}{\partial\alpha}\right|^2 + \int \mathrm{d}^2\alpha P(\alpha)[|\alpha\rangle\langle\alpha|L_\alpha L_\alpha^\dagger] =: \mathcal{F}_P + \mathcal{F}_L. \tag{A11}$$

The evaluation of $\mathcal{F}_L$ is standard but requires careful treatment due to the fact that L_α is ill defined for pure states. The result of such procedure can be found, e.g., in [34–36] and yields

$$\mathcal{F}_L = 1. \tag{A12}$$

For Gaussian prior distribution in Eq. (A1), we calculate

$$\begin{aligned}\mathcal{F}_P &= \int \mathrm{d}^2\alpha P(\alpha)\left|\frac{\partial \ln P(\alpha)}{\partial\alpha}\right|^2 = \int \mathrm{d}^2\alpha P(\alpha)\left|\frac{\partial}{\partial\alpha}\left(-\frac{\alpha_x^2}{\sigma_x^2}-\frac{\alpha_p^2}{\sigma_p^2}\right)\right|^2 \\ &= \int \mathrm{d}^2\alpha \frac{e^{-\frac{\alpha_x^2}{\sigma_x^2}-\frac{\alpha_p^2}{\sigma_p^2}}}{\pi\sigma_x\sigma_p}\left|\frac{\alpha_x}{\sigma_x^2} - i\frac{\alpha_p}{\sigma_p^2}\right|^2 \\ &= \frac{1}{2\sigma_x^2} + \frac{1}{2\sigma_p^2}\end{aligned} \tag{A13}$$

[notice that α and $\alpha*$ are independent variables and $\partial_\alpha(\alpha_x) = \partial_\alpha(\alpha_p) = \frac{1}{2}$]. ∎

Summing the above expressions for $\mathcal{F}_P$ and $\mathcal{F}_L$, one obtains finally

$$\langle|\hat{\alpha} - \alpha|^2\rangle \geq \left(1 + \frac{1}{2\sigma_x^2} + \frac{1}{2\sigma_p^2}\right)^{-1}, \tag{A14}$$

that is the starting bound Eq. (A2) used in the main text Eq. (1).

2. 1-LOCC reduction to local measurements

Consider the situation in which two parameters α and β are independently encoded in the product states

$$\rho(\alpha, \beta) = \rho(\alpha)_A \otimes \rho(\beta)_B. \tag{A15}$$

Here we prove that the minimum estimation error for linear combinations of α and β, under the constraint that measurement is in the 1-LOCC class, main text Eq. (6),

$$\mathcal{M}_{AB}^{(1-\mathrm{LOCC})a,b} = \sum_i p_i \mathcal{M}_A^{(i)a} \otimes \mathcal{M}_B^{(i)b|a}, \tag{A16}$$

by the corresponding combination of minimum errors attained singularly on the two parameters independently, that is,

$$\min_{\mathcal{M}_{AB}^{1-\mathrm{LOCC}}} \langle (f - (c_1\alpha + c_2\beta))^2\rangle = c_1^2 \min_{\mathcal{M}_A} \langle (f_1 - \alpha)^2\rangle + c_2^2 \min_{\mathcal{M}_B} \langle (f_2 - \beta)^2\rangle. \tag{A17}$$

Proof. We explicitly consider the expression to minimize under the 1-LOCC constraint. The estimator f is, in general, a function of the local measurement outputs in Eq. (A16) and possibly the index i. Thus, we have

$$\langle (f - (c_1\alpha + c_2\beta))^2\rangle = \int P(\alpha)P(\beta) \sum_i p_i \sum_a \sum_b [f_i(a,b) - c_1\alpha + c_2\beta]^2 \mathrm{Tr}\left[\left(\mathcal{M}_A^{(i)a} \otimes \mathcal{M}_B^{(i)b|a}\right)(\rho(\alpha)_A \otimes \rho(\beta)_B)\right]. \tag{A18}$$

The first simplification arises from the fact that this expression is an average over the index i, so it must be larger than its minimum addend. Hence, randomizing the AB measurement does not reduce the error. We can therefore restrict ourselves to

$$\langle (f - (c_1\alpha + c_2\beta))^2\rangle \geq \int P(\alpha)P(\beta) \sum_a \sum_b [f(a,b) - c_1\alpha - c_2\beta]^2 \mathrm{Tr}\left[\left(\mathcal{M}_A^{a} \otimes \mathcal{M}_B^{b|a}\right)(\rho(\alpha)_A \otimes \rho(\beta)_B)\right], \tag{A19}$$

which simplifies to

$$\langle (f - (c_1\alpha + c_2\beta))^2\rangle \geq \sum \int P(a,\alpha)P(b,\beta|a)[f(a,b) - c_1\alpha - c_2\beta]^2, \tag{A20}$$

where

$$P(a,\alpha) = P(\alpha)\mathrm{Tr}[\mathcal{M}_A^a \rho(\alpha)_A], \tag{A21}$$

$$P(b,\beta|a) = P(\beta)\mathrm{Tr}\left[\mathcal{M}_B^{b|a} \rho(\beta)_B\right]. \tag{A22}$$

Next, we introduce now the quantity $\bar{f}_\beta(a)$, which represents the average of f over $\{b, \beta\}$ for fixed $\{a\}$:

$$\bar{f}(a) \coloneqq \sum_b \int \mathrm{d}\beta P(b,\beta|a) f(a,b). \tag{A23}$$

Substituting this into the error expression, we can decompose it as

$$\begin{aligned} &\sum \int P(a,\alpha)P(b,\beta|a)(f(a,b) - c_1\alpha - c_2\beta)^2 \\ &= \sum \int P(a,\alpha)P(b,\beta|a)([f(a,b) - \bar{f}(a) + c_2\langle\beta\rangle - c_2\beta]^2 + [\bar{f}(a) - c_1\alpha - c_2\langle\beta\rangle]^2). \end{aligned} \tag{A24}$$

This decomposition is achieved by adding and subtracting $\bar{f}(a) - c_2\langle\beta\rangle$ and recognizing that the cross term averages to zero. Specifically, the cross term $\propto [f(a,b) - \bar{f}(a) + c_2\langle\beta\rangle - c_2\beta][\bar{f}(a) - c_1\alpha - c_2\langle\beta\rangle]$ vanishes due to the successive averaging over b, α and a. Explicitly, we have

$$\sum_a \int \mathrm{d}\alpha P(a,\alpha)(\bar{f}(a) - c_1\alpha - c_2\langle\beta\rangle) \equiv \sum_{a,b} \int \mathrm{d}\alpha\mathrm{d}\beta P(a,\alpha)P(b,\beta|\alpha)(f(a,b) - c_1\alpha - c_2\beta) = 0, \tag{A25}$$

where the second equality holds because $f(a,b)$ can always be assumed to be globally unbiased. This assumption is justified since the average squared error is minimized for globally unbiased estimators. We now define two separate estimators Eq. (A24):

$$f_1(a) \coloneqq \bar{f}(a) - c_2\langle\beta\rangle, \tag{A26}$$

$$f_2(b) \coloneqq f(\tilde{a},b) - \bar{f}(\tilde{a}) + c_2\langle\beta\rangle, \tag{A27}$$

where $\tilde{a}$ is the argument minimizing the residual error:

$$\tilde{a} = \mathrm{argmin}\sum_b \int \mathrm{d}\beta P(b,\beta|a)[f(a,b) - \bar{f}(a) + c_2\langle\beta\rangle - c_2\beta]^2. \tag{A28}$$

Finally, connecting Eq. (A20) with Eq. (A24), with the above definitions, the error can be expressed as

$$\langle[f - (c_1\alpha + c_2\beta)]^2\rangle \geq \langle(f_1 - c_1\alpha)^2 + (f_2 - c_2\beta)^2\rangle. \tag{A29}$$

This confirms that the minimum error is dictated by the independent estimation errors of α and β, weighted by the coefficients c_2^2 and c_2^2, respectively, as desired. ∎

3. Finite-size sampling and Hoeffding bounds for nonresourceful adversaries

Consider now an experiment testing our main inequality Eq. (2) in main text. Given that the quantities $\mathsf{Err}(\gamma_{x,p}) \coloneqq \langle(\hat{\gamma}_{x,p} - \gamma_{x,p})^2\rangle$ are infinite averages, the realization of our proposed protocol instead consists of a finite average of the form

$$\mathsf{Err}[n](\gamma_{x,p}) = \frac{1}{n}\sum_{i=1}^{n}(\hat{\gamma}_{x,p}^{(i)} - \gamma_{x,p}^{(i)})^2. \tag{A30}$$

Clearly, as n grows $\mathsf{Err}[n](\gamma_{x,p}) \to \mathsf{Err}(\gamma_{x,p})$. However, statistical fluctuations may, in principle, allow $\mathsf{Err}[n](\gamma_x) + \mathsf{Err}[n](\gamma_p)$ to violate the bound Eq. (2) in main text. In this Appendix we provide a quantitative bound on the probability of such violation. Namely, under the assumption that Eve is restricted to 1-LOCC measurements [see Methods and Appendix A 2], we want to find a bound of the form

$$P(\mathsf{Err}[n](\gamma_x) + \mathsf{Err}[n](\gamma_p) - (v(\sigma_{x,A},\sigma_{p,A}) + v(\sigma_{x,B},\sigma_{p,B})) < -g) \leq f(g,n) \quad g > 0, \tag{A31}$$

where g quantifies the violation of the bound. For this purpose, we will make use of the Hoeffding inequality.

First, a preliminary observation: we will assume, for simplicity, that Eve performs the same (possibly random) 1-LOCC measurement at each round of the experiment. This is intuitive (the inputs are sampled randomly at each round of the experiment, carry no mutual information $\mathcal{I}(\gamma_{x,p}^{(i)}\colon \gamma_{x,p}^{(j)}) = 0$ for $i \neq j$, and the objective function is an equal average of each round's error), and it is exactly justifiable in the infinite-n limit: as the set of 1-LOCC measurements (and 1-LOCC observables) is convex, and the coherent input coherent states generate i.i.d. random coordinates $\gamma_{x,p}$, any value for $\lim_{n\to\infty}(\mathsf{Err}[n](\gamma_x) + \mathsf{Err}[n](\gamma_p)) = \mathsf{Err}(\gamma_x) + \mathsf{Err}(\gamma_p)$ obtained via different choices of measurements $\mathcal{M}_i$, can be lower-bounded by the minimum expected error $\min_{\mathcal{M}\in\text{1-LOCC}}\mathsf{Err}(\gamma_x) + \mathsf{Err}(\gamma_p)$. In the language of cryptography, we will thus assume "individual attacks" as a reasonable attack strategy for Eve, also in the case of large-but-finite n. We conjecture that a full finite-size cryptographic reduction from coherent attacks to individual attacks could be attainable from applications of the quantum De Finetti theorem [47] to the set of (infinite-dimensional) 1-LOCC POVMs [48,49], or entropy accumulation type theorems [50,51] to the generated correlations, but this is beyond the scope of this work. We thus assume that Eve's measurement $\mathcal{M}_i \equiv \mathcal{M}$ is fixed at each round and that the $\hat{\gamma}_{x,p}^{(i)}$ are i.i.d. distributed.

The Hoeffding inequality states that given a variable x, i.i.d. sampled n times, and bounded such that $a \leq x_i \leq b$, the finitely sampled sum

$$\bar{X}_n \coloneqq \sum_{i=1}^{n} x_i \tag{A32}$$

differs from its expected value $\mathbb{E}[\bar{X}_n] \equiv n\mathbb{E}[x]$ with exponentially small probability, namely,

$$P(\bar{X}_n - n\mathbb{E}[x] \leq t) \leq \exp[-2t^2/(n(b-a)^2)], \tag{A33}$$

which can also be rephrased in terms of the finite-sampled mean $\bar{\mu}_n \coloneqq \bar{X}_n/n$ and $g \coloneqq t/n$ as

$$P(\mu_n - \mu \leq g) \leq \exp[-2ng^2/(b-a)^2]. \tag{A34}$$

For the purpose of our experiment, we take the variable x to be the estimation error at each round of the experiment $x \equiv (\hat{\gamma}_x - \gamma_x)^2 + (\hat{\gamma}_p - \gamma_p)^2$, where $o_{x,p}$ are the estimation outputs (the results of the experiment). It follows that the variable x is always non-negative by definition. Moreover, we can modify the experiment in order not to accept errors that are larger than some cutoff value C. This means in the Hoeffding inequality $a \equiv 0$ and $b \equiv C$. We find that

$$P(\mu_n - \mu \leq g) \leq \exp[-2ng^2/C^2] \tag{A35}$$

as we are interested in "violations in the negative" of our bound, we flip the sign of g as

$$P(\mu_n \leq \mu - g) \leq \exp[-2ng^2/C^2]. \tag{A36}$$

In our case, we do not know the adversarial μ, but we do know from our main inequality Eq. (2) in main text that without quantum resources it has to satisfy

$$\mu \geq v(\sigma_{x,A}, \sigma_{p,A}) + v(\sigma_{x,B}, \sigma_{p,B}) =: \frac{2\sigma^{*2}}{\sigma^{*2}+1}. \tag{A37}$$

Therefore, we can upper bound the probability of violating the witness by an amount g via the inequality that follows:

$$P\left(\mu_n \leq \frac{2\sigma^{*2}}{\sigma^{*2}+1} - g\right) \leq P(\mu_n \leq \mu - g) \leq \exp[-2ng^2/C^2]. \tag{A38}$$

a. Evaluation on the experimental output

We evaluate the Hoeffding inequality using the experimental results. In the entanglement-witness experiment, we have $n = 1000$, and the values of g (corresponding to the observed violations of the MDIEW bound in the main text) together with the associated probabilities of violation for different distribution widths are presented in Table I. As expected, the smallest probability is observed for the largest coherent-state distribution, where the bound is tighter, yielding a probability below 5%.

TABLE I. Values of distribution size σ^*, magnitude of violation of the nonentanglement bound and the probability of violation, for the entanglement witness experiment. Entries of $\cdots$ is where the value of the witness is above the MDI bound.

σ^*	0	0.74	1.76	3.26	5.64	6.49
g	$\cdots$	$\cdots$	$\cdots$	0.050	0.125	0.165
P	$\cdots$	$\cdots$	$\cdots$	73%	15.6%	4.2%

TABLE II. Values of distribution size σ^*, magnitude of violation of the nonentanglement bound and the probability of violation, for the memory certification experiment. The entry of $\cdots$ is where the value of the witness is above the MDI bound.

σ^*	1.01	1.62	1.76	2.22
g	$\cdots$	0.212	0.209	0.199
P	$\cdots$	≈ 0	≈ 0	≈ 0

For the memory experiment, we have a much larger number of states, 2×10^6. The probability of violation derived from the Hoeffding inequality is effectively zero (on the order of 10^{-100}) as shown in Table II.

As seen, the probability of violation is significantly lower for the memory experiment, primarily due to the larger number of states and the exponential dependence of the Hoeffding bound on the number of measurements. The ability to generate a larger number of unique coherent states in the memory experiment arises simply from its specific technical implementation.

APPENDIX B: EXPERIMENTAL DETAILS

Detailed schematics of the setup can be seen for entanglement witness in Fig. 5 and for memory certification in Fig. 6.

1. Entanglement witness: Coherent state generation

To calibrate the relationship between the amplitude of the resulting amplitude of generated coherent states, we varied the modulation voltage while measuring only the generated coherent states. A clear linear relationship was observed (Fig. 8), allowing Alice and Bob to accurately generate known coherent states for the trusted input.

Coherent states for both Alice and Bob were generated using the same method. IM and PM from "iXblue" were used to modulate α_x and α_p components of the states, respectively. The coherent states were generated at a sideband frequency of $S_{\text{meas}} = 3.1$ MHz. By varying the modulation voltage, coherent states with different amplitudes were generated in the sideband. In addition, the IM and PM generated sidebands at $S_x = 31$ and $S_p = 41$ MHz, respectively, which were used to lock the homodyne detectors to the x and p quadratures. The RedPitaya boards running

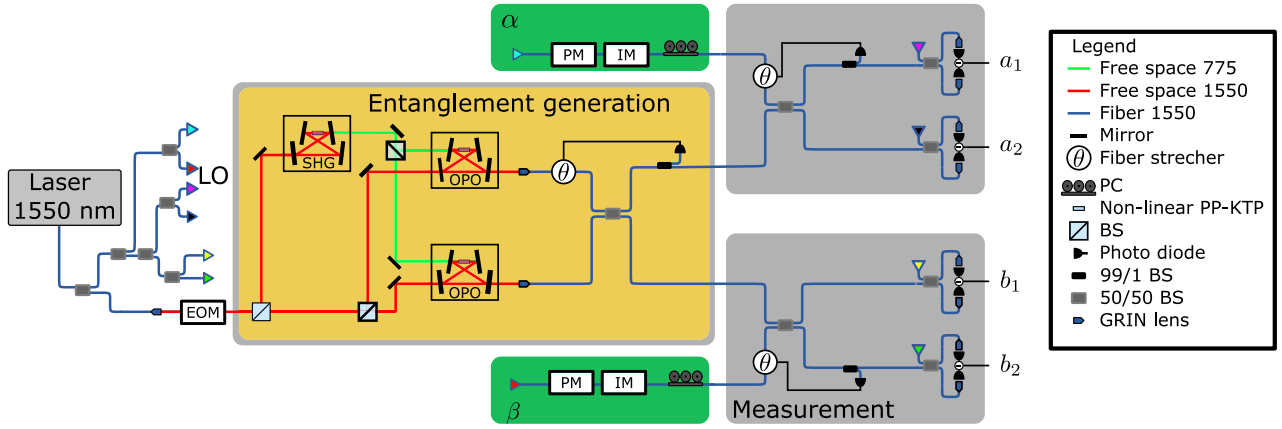


FIG. 5. Detailed schematic of the setup for the generation of entangled two-mode squeezed vacuum state, coherent state generation and measurement.

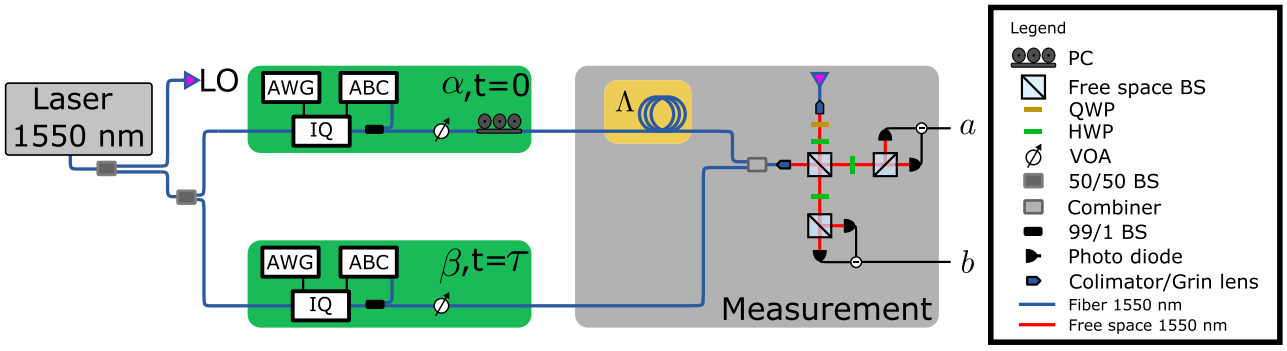


FIG. 6. Experimental setup for quantum memory certification.

PYRPL software were used for generating the states and locking signals.

For the experimental alphabet, 1000 coherent states were randomly generated from a Gaussian distribution. A sample of these states is shown in Fig. 7, with scatter plots and histograms illustrating the x and p quadratures for Alice and Bob.

The phase between the coherent states and the TMSV was locked after interference at a 50/50 BS. This was achieved using a 99/1 BS in one arm to monitor

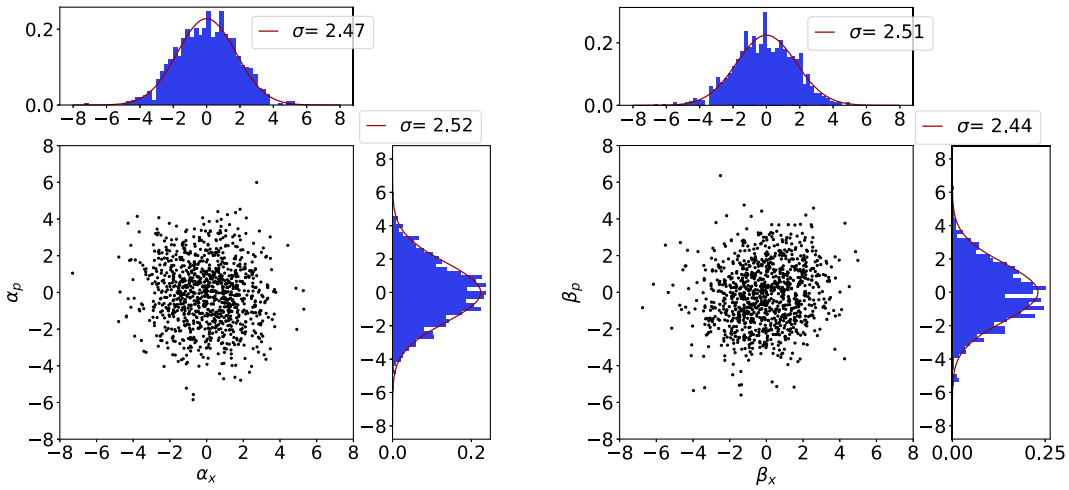


FIG. 7. Scatter plots and histograms of the $\hat{x}$ and $\hat{p}$ quadrature for the 1000 states generated with $\sigma \approx 2.5$. Left: Alice's states. Right: Bob's states.

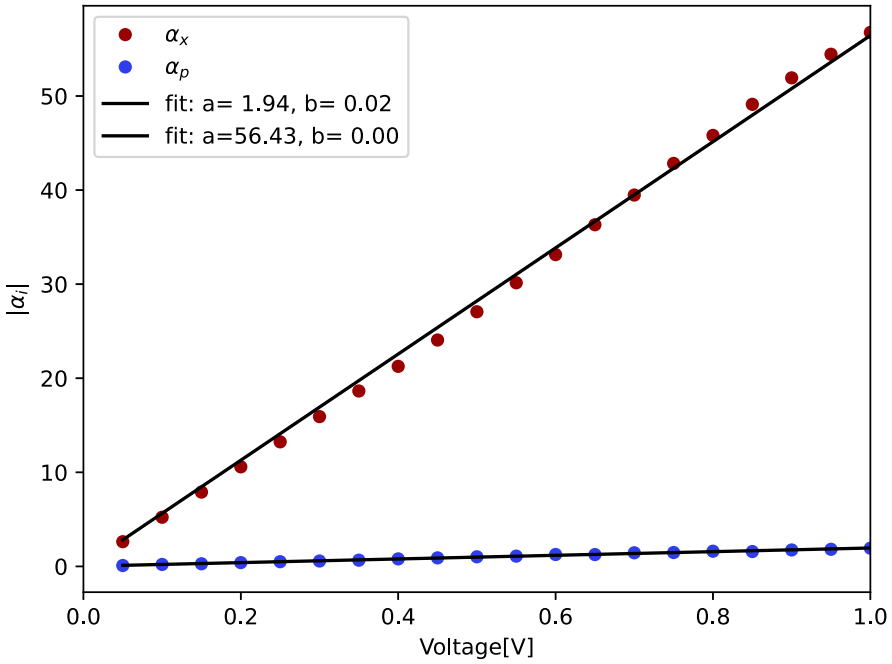


FIG. 8. Linear relationship between the modulation voltage applied to the phase modulator and the amplitude of the generated state in the $\hat{p}$ quadrature. Additionally, a linear dependence is observed in the $\hat{x}$ quadrature, indicating residual modulation. This behavior highlights the need for compensation when generating coherent states with precise quadrature control.

the phase, and a fiber stretcher before the 50/50 BS to apply corrections.

During calibration, we found that generating a coherent state using only the IM, intended to produce amplitude modulation in the $\hat{x}$ quadrature, also introduced a small residual modulation in the $\hat{p}$ quadrature, and vice versa. This effect is likely due to residual amplitude modulation caused by the crystal's response to the modulation frequency [52]. Fortunately, this response scales linearly with the amplitude modulation (see Fig. 8), allowing us to account for it when generating the coherent state alphabet. By applying a compensating modulation through the PM, we effectively canceled the unintended modulation in $\hat{p}$ from the IM, enabling independent generation of any desired coherent state.

2. Entanglement witness: Efficiency budget

In this section, we analyze the efficiency of the setup, focusing on state generation, transmission of the state to the detectors and the detection efficiency. For state generation, the escape efficiencies of the optical parametric oscillators (OPOs) were measured as $97.5 \pm 0.1\%$ (intracavity loss: 0.255%) for OPO 1, and $94.4 \pm 0.1\%$ (intracavity loss 0.588%) for OPO 2. The coupling efficiencies of the OPO outputs into the fibers were $87 \pm 1\%$ and $84 \pm 1\%$, respectively.

The optical transmission in the fiber components includes losses from two 50/50 fiber couplers (used for generating the EPR state and mixing the coherent states), a 99/1 fiber coupler for tapping light for locking, fiber splicing and fiber absorption. The total transmission efficiencies to the 4 homodyne detectors were measured as 20%, 22%, 21%, and 21% for homodynes 1, 2, 3, and 4, respectively.

The detector efficiency of each homodyne detector is determined by the diode efficiency (99%, form spec sheet), visibility (optimized through fiber coupling for spatial mode matching), and electronic noise clearance (98%–99% with a signal-to-noise ratio of 18–20 dB). The resulting detection efficiencies were 95%, 96%, 94%, and 95% for homodynes 1, 2, 3, and 4, respectively.

Using the efficiencies from state generation, transmission, and detection, we calculated the expected squeezing levels. For the total efficiency η, the bandwidth of the cavity $\Omega = 8.35$ MHz, the sideband frequency of the measurement $\Omega = 3.1$ MHz, and $\zeta = \Omega\sqrt{P/P_{\text{thr}}}$, where $(P/P_{\text{thr}}) \approx 0.40$ (with P and P_{thr} being the pump and threshold power), we find

$$\begin{aligned}\langle \Delta^2(\hat{x}_1 - \hat{x}_2)\rangle &= \langle \Delta^2(\hat{p}_1 + \hat{p}_2)\rangle \\ &= \frac{1}{2} - 2\eta\frac{\Omega\zeta}{(\Omega+\zeta)^2+\omega^2} \approx 0.42, \\ \langle \Delta^2(\hat{x}_1 + \hat{x}_2)\rangle &= \langle \Delta^2(\hat{p}_1 - \hat{p}_2)\rangle \\ &= \frac{1}{2} + 2\eta\frac{\Omega\zeta}{(\Omega+\zeta)^2+\omega^2} = 1.38.\end{aligned}$$

For measurements with $\sigma = 0$, the observed squeezing levels were

$$\langle \Delta^2(\hat{x}_1 - \hat{x}_2)\rangle = 0.428 \pm 0.019,$$
$$\langle \Delta^2(\hat{x}_1 + \hat{x}_2)\rangle = 1.206 \pm 0.068,$$
$$\langle \Delta^2(\hat{p}_1 + \hat{p}_2)\rangle = 0.417 \pm 0.019,$$
$$\langle \Delta^2(\hat{p}_1 - \hat{p}_2)\rangle = 1.429 \pm 0.063.$$

The measured squeezing was slightly lower than the expected, while the antisqueezing was slightly higher. Introducing an additional 20% loss in the calculations aligns the expected squeezing with the observed values, giving $S = 0.43$ for squeezing and $AS = 1.20$ for antisqueezing. This suggests the presence of an unknown loss in the system.

3. Squeezing-loss analysis for TMSV

We analyze the proposed experimental protocol for MDI entanglement witnessing, schematically depicted in Fig. 9. By taking the outputs $a_1 - b_1$ and $a_2 + b_2$ as estimators for $\alpha_x - \beta_x$ and $\alpha_p + \beta_p$, respectively, the MDI witness value from Eq. (2) in main text becomes

$$\langle \mathrm{MDIEW}\rangle = \langle (a_1 - b_1 - (\alpha_x - \beta_x))^2\rangle + \langle (a_2 + b_2 - (\alpha_p + \beta_p))^2\rangle \tag{B1}$$

$$= \left\langle \left(\frac{\hat{x}_A + \hat{x}_a - \hat{x}_B - \hat{x}_b}{\sqrt{2}} - (\alpha_x - \beta_x) \right)^2 \right\rangle + \left\langle \left(\frac{\hat{p}_A - \hat{p}_a + \hat{p}_B - \hat{p}_b}{\sqrt{2}} - (\alpha_p + \beta_p) \right)^2 \right\rangle. \tag{B2}$$

Now, consider the source ρ_{AB} as a two-mode squeezed vacuum. Using the properties of TMSV, we know that $\langle \hat{x}_A\rangle = \langle \hat{p}_A\rangle = \langle \hat{x}_B\rangle = \langle \hat{p}_B\rangle = 0$, as well as $\langle \hat{x}_a\rangle = \sqrt{2}\alpha_x$, $\langle \hat{x}_b\rangle = \sqrt{2}\beta_x$ (and similarly for $\hat{p}$). Substituting these into the above expression, we simplify

$$\langle \mathrm{MDIEW}\rangle = \frac{1}{2}(\langle (\hat{x}_A - \hat{x}_B)^2\rangle + \Delta\hat{x}_a^2 + \Delta\hat{x}_b^2 + \langle (\hat{p}_A + \hat{p}_B)^2\rangle + \Delta\hat{p}_a^2 + \Delta\hat{p}_b^2) \tag{B3}$$

$$= 1 + \frac{1}{2}(\langle (\hat{x}_A - \hat{x}_B)^2\rangle + \langle (\hat{p}_A + \hat{p}_B)^2\rangle). \tag{B4}$$

For a TMSV with squeezing parameter r, we have $\langle (\hat{x}_A - \hat{x}_B)^2\rangle + \langle (\hat{p}_A + \hat{p}_B)^2\rangle = 2e^{-2r}$. Substituting this result, the MDI witness evaluates to $\langle \mathrm{MDIEW}\rangle = 1 + e^{-2r}$, which is strictly less than 2 for any nonzero squeezing $r > 0$, confirming the presence of entanglement.

Optical losses in the TMSV can be modeled as a beam splitter with transmissivity η (we are assuming same loss in both channels). The modes transform as

$$\{\hat{x}_A, \hat{p}_A, \hat{x}_B, \hat{p}_B\} \to \sqrt{\eta}\{\hat{x}_A, \hat{p}_A, \hat{x}_B, \hat{p}_B\} + \sqrt{1-\eta}\{\hat{x}_{V_A}, -\hat{p}_{V_A}, \hat{x}_{V_B}, -\hat{p}_{V_B}\},$$

where V_A and V_B are channel modes. After the loss channel the witness becomes

$$\langle \mathrm{MDIEW}\rangle = 1 + \eta e^{-2r} + (1-\eta)(1+\xi), \tag{B5}$$

where $1/2(1+\xi)$ is the noise of the channel modes. If the channel is vacuum we get $\xi = 0$:

$$\langle \mathrm{MDIEW}\rangle = 2 + \eta(e^{-2r} - 1), \tag{B6}$$

This expression shows that losses reduce the effectiveness of the witness. We plot the resulting value of $\langle \mathrm{MDIEW}\rangle$ as a function of η and r in Fig. 12(a). The plot illustrates the critical interplay between squeezing and losses, demonstrating that the witness remains below the threshold for sufficiently high η and $r > 0$.

4. Rescaling of measurements by Eve

A rescaling of measurements, either due to experimental errors or intentional tampering by Eve, can lead to false violation of the Simon-Duan criterion. For example, a separable vacuum state can erroneously violate this criterion when the measurements are multiplied by a rescaling factor $\epsilon < 1$.

$$\langle \mathrm{EW}\rangle = \langle \Delta^2(\hat{x}_1 - \hat{x}_2)\rangle + \langle \Delta^2(\hat{p}_1 + \hat{x}_2)\rangle = 2 \to,$$
$$\langle \mathrm{EW}\rangle(\epsilon) = \langle \Delta^2(\epsilon\hat{x}_1 - \epsilon\hat{x}_2)\rangle + \langle \Delta^2(\epsilon\hat{p}_1 + \epsilon\hat{x}_2)\rangle$$
$$= 2\epsilon^2 < 2.$$

For the MDI protocol, Eve estimates the coherent states sent by Alice and Bob by mixing the states $\hat{x}_a$ with her state $\hat{x}_A$ using a 50/50 BS and measuring the $\hat{x}$ and $\hat{p}$ quadratures of the outputs (see Fig. 9). For a rescaling attack, Eve multiplies her measurement outcomes $\{a_1, a_2, b_1, b_2\}$ by the factor ϵ.

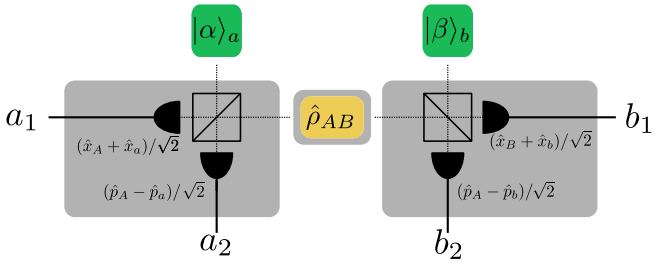


FIG. 9. Eve's measurement setup. In the rescaling attack, Eve multiplies here measurement outcomes $\{a_1, a_2, b_1, b_2\}$ with the rescaling factor ϵ. The MDI witness ensures that only if the state $\hat{\rho}_{AB}$ is entangled can Eve violate the bound in Eq. (2) in main text, even with rescaling.

With this setup, with a rescaling by ϵ, the error ($\mathsf{Err}(\gamma_x)$) becomes

$$\langle\mathcal{E}\rangle(\epsilon)_x \equiv \left\langle \left(\frac{\epsilon}{\sqrt{2}}(\hat{x}_a+\hat{x}_A-\hat{x}_b-\hat{x}_B)-(\alpha_x-\beta_x)\right)^2\right\rangle \tag{B7}$$

$$\underbrace{=}_{\langle\hat{x}_A\rangle=\langle\hat{x}_B\rangle=0} \frac{\epsilon^2}{2}\langle\hat{x}_a^2+\hat{x}_A^2+\hat{x}_b^2+\hat{x}_B^2\rangle+\alpha_x^2+\beta_x^2-\epsilon^2\langle\hat{x}_A\hat{x}_B\rangle \tag{B8}$$

$$-\epsilon^2\langle\hat{x}_a\rangle\langle\hat{x}_b\rangle-\sqrt{2}\epsilon\alpha_x\langle\hat{x}_a\rangle+\sqrt{2}\epsilon\alpha_x\langle\hat{x}_b\rangle+\sqrt{2}\epsilon\beta_x\langle\hat{x}_a\rangle \tag{B9}$$

$$-\sqrt{2}\epsilon\beta_x\langle\hat{x}_b\rangle+2\alpha_x\beta_x. \tag{B10}$$

Using $\langle\hat{x}_a\rangle=\sqrt{2}\alpha_x$ and $\langle\hat{x}_b\rangle=\sqrt{2}\beta_x$, we find

$$\langle\mathcal{E}\rangle(\epsilon)_x=\left\langle\left(\frac{\epsilon}{\sqrt{2}}(\hat{x}_a+\hat{x}_A-\hat{x}_b-\hat{x}_B)-(\alpha_x-\beta_x)\right)^2\right\rangle=\frac{\epsilon^2}{2}\langle(\hat{x}_A-\hat{x}_B)^2\rangle$$
$$+\epsilon^2\left(\alpha_x^2+\beta_x^2+\frac{1}{2}\right)+\alpha_x^2+\beta_x^2-2\epsilon^2\beta_x\alpha_x+2\epsilon(2\alpha_x\beta_x-\alpha_x^2-\beta_x^2)+2\alpha_x\beta_x.$$

For many coherent states from a distribution with variance $2\sigma^{*2}$ we get

$$\langle\mathcal{E}\rangle(\epsilon)_x=\left\langle\left(\frac{\epsilon}{\sqrt{2}}(\hat{x}_a+\hat{x}_A-\hat{x}_b-\hat{x}_B)-(\alpha_x-\beta_x)\right)^2\right\rangle$$
$$=\frac{\epsilon^2}{2}\langle(\hat{x}_A-\hat{x}_B)^2\rangle+\frac{\epsilon^2}{2}+\sigma^{*2}(\epsilon-1)^2,$$

where we used that the distributions are centered around zero so $\mathrm{mean}(\alpha_x)=\mathrm{mean}(\beta_x)=0$.

For $\langle\mathcal{E}\rangle(\epsilon)_p$ we proceed in a similar way, so in total we get

$$\langle\mathcal{E}\rangle(\epsilon)=\langle\mathcal{E}\rangle(\epsilon,r)_x+\langle\mathcal{E}\rangle(\epsilon)_p=\frac{\epsilon^2}{2}(\langle(\hat{x}_A-\hat{x}_B)^2+(\hat{p}_A+\hat{p}_B)^2\rangle)+\epsilon^2+2\sigma^{*2}(\epsilon-1)^2. \tag{B11}$$

If Eve has access to a TMSV state with squeezing $\langle(\hat{x}_A-\hat{x}_B)^2\rangle+\langle(\hat{p}_A+\hat{p}_B)^2\rangle=2\mathrm{e}^{-2r}<2$ for $r>0$, the error becomes

$$\langle\mathcal{E}\rangle(\epsilon,r)=\epsilon^2\mathrm{e}^{-2r}+\epsilon^2+2(\epsilon-1)^2\sigma^{*2}. \tag{B12}$$

For $r=0$, the state is separable, and Eve can only saturate the MDI bound without violating it.

To find Eve's optimal rescaling factor ϵ_{opt}, we minimize the error:

$$\frac{\mathrm{d}}{\mathrm{d}\epsilon}\langle\mathcal{E}\rangle(\epsilon,r)=2\epsilon\mathrm{e}^{-2r}+2\epsilon+4(\epsilon-1)\sigma^{*2}=0,$$

yielding

$$\epsilon_{\mathrm{opt}}=\frac{2\sigma^{*2}}{2\sigma^{*2}+\mathrm{e}^{-2r}+1}.$$

For a separable state ($r=0$), the resulting error is

$$\langle\mathcal{E}\rangle(\epsilon_{\mathrm{opt}},0)=2\epsilon_{\mathrm{opt}}^2+2(\epsilon_{\mathrm{opt}}-1)^2\sigma^{*2}=\frac{2\sigma^{*2}}{\sigma^{*2}+1},$$

which matches the MDI bound $2v(\sigma^*,\sigma^*)$, ensuring Eve cannot falsely detect entanglement.

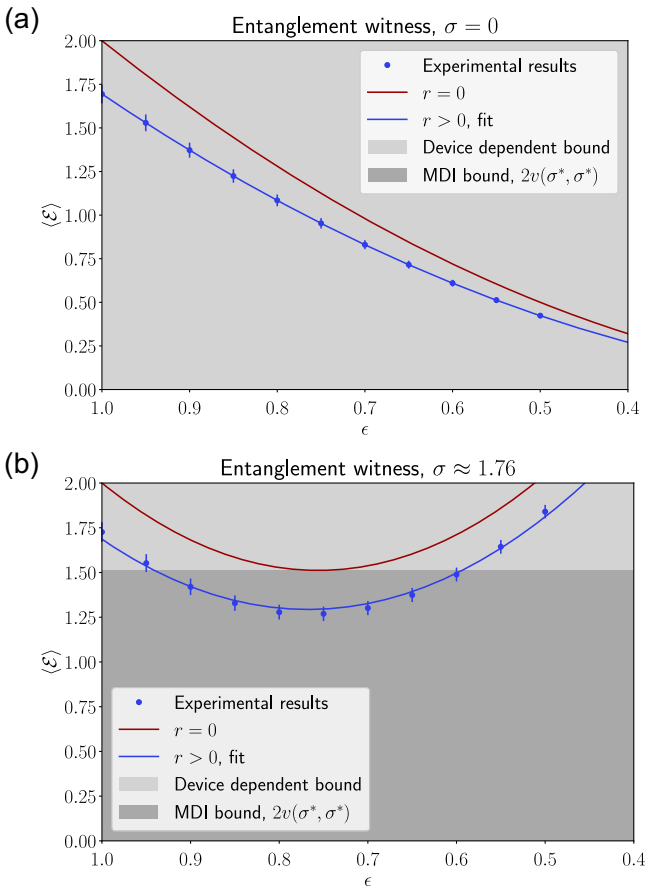


FIG. 10. (a) For separable states ($r = 0$), rescaling $\epsilon < 1$ can lead to false violations of the Simon-Duan criterion. (b) For intermediate σ, rescaling by Eve saturates but does not violate the MDI bound. Entanglement ($r < 1$) allows the MDI bound to be violated as expected.

For Eve's rescaling, where the output is modified as $a_1 = \epsilon[(\hat{x}_a + \hat{x}_A)/\sqrt{2}]$, the predictions of the coherent states sent by Alice become inaccurate. This leads to an increase in the value of $\langle \mathcal{E} \rangle(\epsilon, r)$ when the measurements are rescaled. Thus, for lower values of ϵ, the value of $\langle \mathcal{E} \rangle(\epsilon, r)$ increases. Eve's choice of ϵ involves a trade-off: reducing variance while maintaining the ability to correctly estimate the coherent states. This trade-off is evident in Fig. 4(a), which compares the effects of rescaling for a separable vacuum state ($r = 0$, red line) and entangled TMSV state ($r > 0$, blue line).

Without the trusted information held by Alice and Bob ($\sigma = 0$), Eve can exploit rescaling to decrease the value of $\langle \mathcal{E} \rangle(\epsilon, r)$, potentially violating the device-dependent Simon-Duan bound with a separable state. However, the MDI bound $2v(\sigma^*, \sigma^*) = 0$ remains secure: even with an entangled TMSV state, it cannot be violated. This is depicted for varying ϵ in Fig. 10(a). In Fig. 10(a), we consider a scenario where Alice and Bob generate coherent states from a distribution with $\sigma^* \approx 1.76$. In this case, the value of $\langle \mathcal{E} \rangle(\epsilon, r = 0)$ decreases for small values of ϵ. However, due to the trade-off between accurately predicting coherent states and reducing variance in Eve's homodyne measurements, the minimum value that Eve can achieve saturates the MDI bound but cannot violate it. For the case of nonzero squeezing ($r > 0$), the MDI bound can be violated, as expected, due to the presence of both a nonseparable state and additional information known only to Alice and Bob.

The regions in which the MDI bound can be violated, determined by $\langle \mathcal{E} \rangle(\epsilon, r) - 2v(\sigma, \sigma) \geq 0$, are shown in Fig. 11.

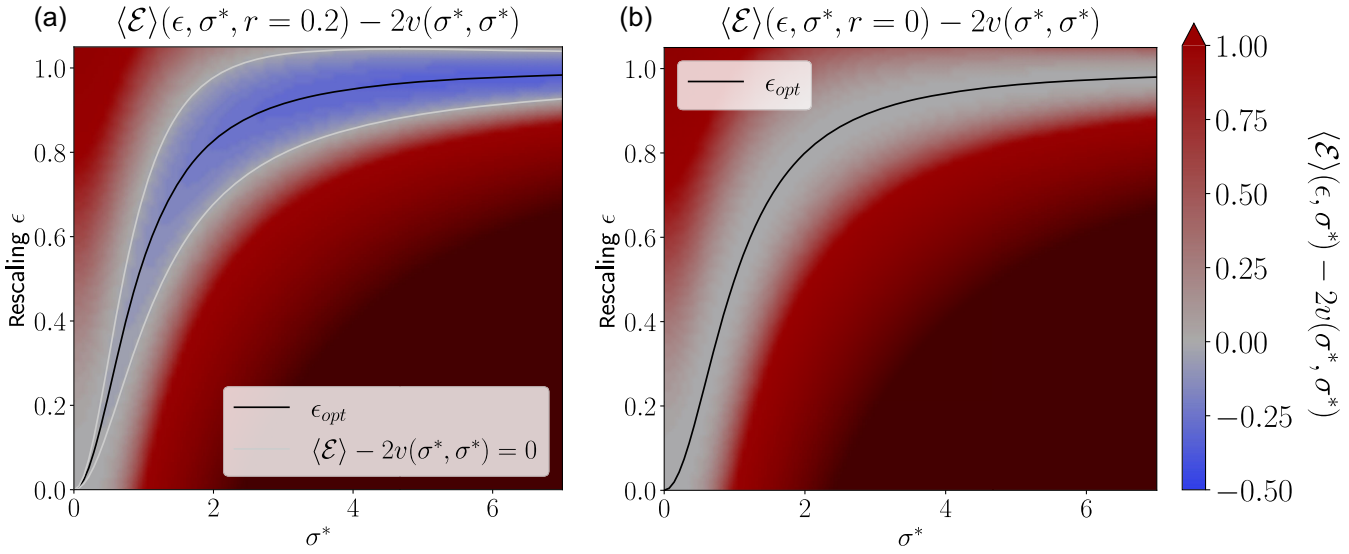


FIG. 11. Contour plots of $\langle \mathcal{E} \rangle(\epsilon, r) - 2v(\sigma, \sigma)$ for (a) $r = 0.2$ and (b) $r = 0$. Regions where $\langle \mathcal{E} \rangle(\epsilon, r) - 2v(\sigma, \sigma) < 0$ indicate successful entanglement detection. For a separable state ($r = 0$), as shown in (b), the MDI bound cannot be violated even with shot noise rescaling ($\epsilon \neq 1$). However, for squeezed states ($r = 0.2$), as shown in (a), the bound can be violated, demonstrating the presence of entanglement.

APPENDIX C: MEMORY WITNESSING

If we model the memory as a lossy channel with transmission efficiency η and excess noise ξ, the output quadrature after passing through the memory is given by

$$\hat{x}'_a = \sqrt{\eta}\hat{x}_a + \sqrt{1-\eta}\hat{x}_{00},$$

where $\langle \Delta^2 \hat{x}_{00} \rangle = [(1+\xi)/2]$. To correctly estimate the input coherent state, Eve might need to amplify output of the channel. After amplification by a gain factor ν, the output quadrature becomes

$$\hat{x}''_a = \sqrt{\nu}\hat{x}'_a + \sqrt{\nu-1}\hat{x}_{01} = \sqrt{\nu\eta}\hat{x}_a + \sqrt{\nu(1-\eta)}\hat{x}_{00} + \sqrt{\nu-1}\hat{x}_{01},$$

To match the state $|\beta_{t=\tau}\rangle$ with the state $|\alpha_{t=0}\rangle$, a similar scaling is applied:

$$\hat{x}'_b = \sqrt{\eta\nu}\hat{x}_b + \sqrt{1-\eta\nu}\hat{x}_{02}.$$

Eve then estimates the coherent state by performing homodyne detection and scaling the measurement outcome by $1/\sqrt{\nu\eta}$:

$$\hat{a} = \frac{\hat{x}''_a + \hat{x}'_b}{\sqrt{2\nu\eta}},$$

and similarly for the $\hat{p}$ quadrature.

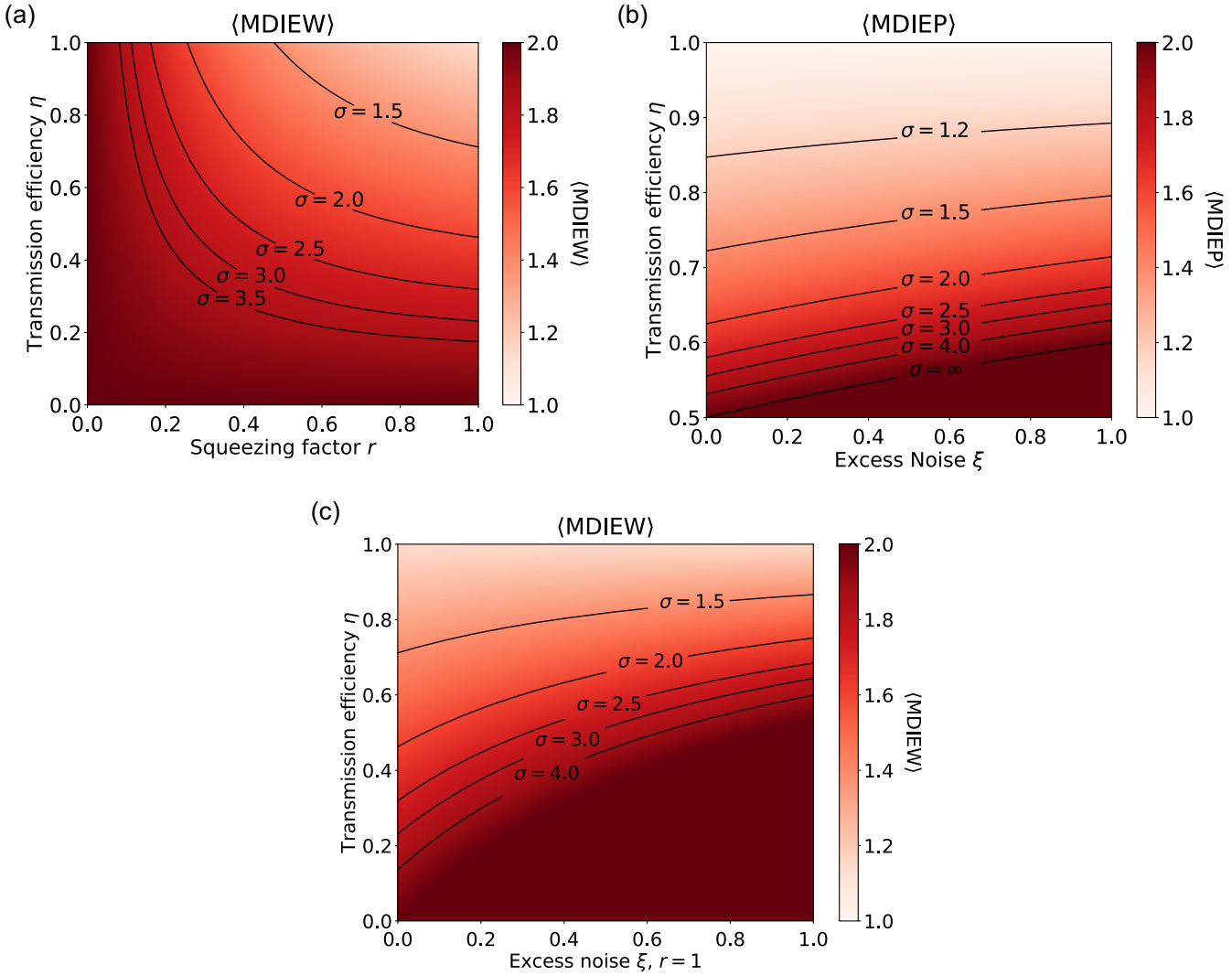


FIG. 12. (a) Contour plot showing the values of ⟨MDIEW⟩ achievable for different squeezing levels r and transmission efficiencies η. The contours represent the values of σ required to violate the bound $\langle \text{MDIEW} \rangle \geq 2v(\sigma,\sigma)$, for no excess noise $\xi = 0$ (b) Contour plot of the values of ⟨MDIEP⟩ achievable for different values of transmission efficiency η and excess noise ξ. The contours indicate the values of σ needed to violate the bound $\langle \text{MDIEP} \rangle \geq 2v(\sigma,\sigma)$. (c) Contour plot showing the values of ⟨MDIEW⟩ achievable for different transmission efficiency η and excess noise ξ in the loss channel. The contours represent the values of σ required to violate the bound $\langle \text{MDIEW} \rangle \geq 2v(\sigma,\sigma)$.

The memory witness is evaluated as follows:

$$\begin{aligned}\langle \mathrm{MDIEP}\rangle &= \langle(\hat{a}-\alpha_x-\beta_x)^2\rangle + \langle(\hat{b}_p-\alpha_p+\beta_p)^2\rangle \\ &= \langle\hat{a}^2\rangle - 2\langle\hat{a}\rangle\underbrace{(\alpha_x+\beta_x)}_{=\langle\hat{a}\rangle} + (\alpha_x+\beta_x)^2 \\ &\quad + \langle(\hat{b}-\alpha_p+\beta_p)^2\rangle \\ &= \langle\hat{a}^2\rangle - \langle\hat{a}\rangle^2 + \langle\hat{b}^2\rangle - \langle\hat{b}\rangle^2 = \langle\Delta^2\hat{a}\rangle + \langle\Delta^2\hat{b}\rangle. \end{aligned} \tag{C1}$$

We can now evaluate the variance of $\hat{a}$:

$$\begin{aligned}\langle\Delta^2\hat{a}\rangle &= \frac{1}{2\nu\eta}\langle\hat{x}_a''-\hat{x}_b'\rangle^2 \\ &= \frac{1}{2\nu\eta}(\eta\nu\langle\Delta^2\hat{x}_a\rangle + \nu(1-\eta)\langle\Delta^2\hat{x}_{00}\rangle \\ &\quad + (\nu-1)\langle\Delta^2\hat{x}_{01}\rangle + \nu\eta\langle\Delta^2\hat{x}_p\rangle + (1-\nu\eta)\langle\Delta^2\hat{x}_{02}\rangle) \\ &= \frac{1}{4\nu\eta}(\eta\nu + \nu(1-\eta)(1+\xi) + \nu - 1 + \eta\nu + 1 - \eta\nu) \\ &= \frac{1}{4\eta}(2+\xi+\eta\xi),\end{aligned}$$

and similarly, for $\langle\Delta^2\hat{b}\rangle$. By combining these results, we find

$$\langle \mathrm{MDIEP}\rangle = \frac{1}{2\eta}(2+\xi+\eta\xi), \tag{C2}$$

which reduces to $\langle \mathrm{MDIEP}\rangle = (1/\eta)$ for $\xi = 0$.

The witness does not depend on the gain factor ν, performed in postprocessing. The values of $\langle \mathrm{MDIEP}\rangle$ for varying η and ξ are shown in Fig. 12(b).

APPENDIX D: PHASE NOISE MODEL

We now examine the impact of phase noise in the experimental setup. Three types of phase noise need to be considered: (i) Phase between the to SMSV states during the preparation of the TMSV state. (ii) Phase noise between the TMSV and the detectors. (iii) Phase noise between the coherent states and the detectors. To simplify the analysis, we assume that the phase noise is consistent across both modes of the TMSV and all four detectors, as well as across both coherent states and all four detectors.

We model phase noise as random phase shifts. A phase shift θ_1 represents the phase noise between the TMSV and the homodyne detectors, while θ_2 represents the phase noise between the coherent states and the detectors. The quadrature transformations are expressed as

$$\begin{aligned}\hat{x}_A &\to \cos(\theta_1)\hat{x}_A + \sin(\theta_1)\hat{p}_A, \\ \hat{p}_A &\to \cos(\theta_1)\hat{p}_A - \sin(\theta_1)\hat{x}_A, \\ \hat{x}_a &\to \cos(\theta_2)\hat{x}_a + \sin(\theta_2)\hat{p}_a, \\ \hat{p}_a &\to \cos(\theta_2)\hat{p}_a - \sin(\theta_2)\hat{x}_a,\end{aligned}$$

and similarly for $\hat{x}_B, \hat{p}_B, \hat{x}_b$, and $\hat{p}_b$. Additionally, We account for transmission losses, assuming for simplicity that $\eta_A = \eta_B$.

Next, we consider a phase shift of θ_3 between the two modes of the SMSV, leading to the following transformation:

$$\begin{aligned}\langle\hat{x}_A^2\rangle &= \cosh(2r)/2 \to \langle\hat{x}_A^2\rangle = \cosh(2r)/2, \\ \langle\hat{x}_B^2\rangle &= \langle\hat{p}_A^2\rangle = \langle\hat{p}_B^2\rangle, \\ \langle\hat{x}_A\hat{x}_B\rangle &= \sinh(2r)/2 \to \langle\hat{x}_A\hat{x}_B\rangle = \cos(\theta_3)\sinh(2r)/2, \\ \langle\hat{x}_A\hat{x}_B\rangle &= -\langle\hat{p}_A\hat{p}_B\rangle, \\ \langle\hat{x}_A\hat{p}_B\rangle &= 0 \to \langle\hat{x}_A\hat{p}_B\rangle = -\sin(\theta_3)\sinh(2r)/2, \\ \langle\hat{p}_A\hat{x}_B\rangle &= \langle\hat{x}_A\hat{p}_B\rangle.\end{aligned}$$

Substituting these transformations into the error expression, we find

$$\begin{aligned}\langle\mathcal{E}\rangle(\epsilon,r,\eta,\theta_1,\theta_2,\theta_3) &= \epsilon^2\eta(\cos^2(\theta_1)(\cosh(2r)-\cos(\theta_3)\sinh(2r)) - \sin^2(\theta_1)(\cosh(2r)+\cos(\theta_3)\sinh(2r)) \\ &\quad + 2\cos(\theta_1)\sin(\theta_1)\sin(\theta_3)\sinh(2r)) + (1-\eta)\epsilon^2 + \epsilon^2 + 2\sigma^2(1+\epsilon^2-2\epsilon\cos(\theta_2)).\end{aligned}$$

For phase noise modeled as Gaussian-distributed random variables with variances $\Delta^2\theta_1, \Delta^2\theta_2$, and $\Delta^2\theta_3$, the average becomes [53]

$$\begin{aligned}&\langle\mathcal{E}\rangle(\epsilon,r,\eta,\Delta^2\theta_1,\Delta^2\theta_2,\Delta^2\theta_3) \\ &= \int_{-\infty}^{\infty}\mathrm{d}\theta_1\mathrm{d}\theta_2\mathrm{d}\theta_3\,\frac{1}{\sqrt{2\pi\Delta^2\theta_1}}\frac{1}{\sqrt{2\pi\Delta^2\theta_2}}\frac{1}{\sqrt{2\pi\Delta^2\theta_3}}\mathrm{e}^{-\theta_1^2/(2\Delta^2\theta_1)}\mathrm{e}^{-\theta_2^2/(2\Delta^2\theta_2)}\mathrm{e}^{-\theta_3^2/(2\Delta^2\theta_3)}\langle\mathrm{MDIEW}\rangle(\epsilon,r,\eta,\theta_1,\theta_2,\theta_3) \\ &= \epsilon^2\eta\left[\frac{1+\mathrm{e}^{-2\Delta^2\theta_1}}{2}\{\cosh(2r)-\mathrm{e}^{-\Delta^2\theta_3/2}\sinh(2r)\} + \frac{1-\mathrm{e}^{-2\Delta^2\theta_1}}{2}\{\cosh(2r)+\mathrm{e}^{-\Delta^2\theta_3/2}\sinh(2r)\}\right] \\ &\quad + (1-\eta)\epsilon^2 + \epsilon^2 + 2\sigma^2(1+\epsilon^2-2\epsilon\mathrm{e}^{-\Delta^2\theta_2/2}).\end{aligned}$$

Without phase noise and assuming $\epsilon = 1$, the error reduces to

$$\langle \mathcal{E} \rangle (1, r, \eta, 0, 0, 0) = \langle \mathrm{MDIEW} \rangle = 2 + \eta(\mathrm{e}^{-2r} - 1).$$

The corresponding values can be visualized in Fig. 12(a). With phase noise, the error includes the effects of phase noise, leading to a decrease in the observed squeezing and consequently affecting the ability to witness entanglement.

[1] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, and E. Kashefi, *Quantum certification and benchmarking*, Nat. Rev. Phys. **2**, 382 (2020).

[2] M. Kliesch and I. Roth, *Theory of quantum system certification*, PRX Quantum **2**, 010201 (2021).

[3] A. I. Lvovsky and M. G. Raymer, *Continuous-variable optical quantum-state tomography*, Rev. Mod. Phys. **81**, 299 (2009).

[4] J.-D. Bancal, N. Gisin, Y.-C. Liang, and S. Pironio, *Device-independent witnesses of genuine multipartite entanglement*, Phys. Rev. Lett. **106**, 250404 (2011).

[5] F. Baccari, D. Cavalcanti, P. Wittek, and A. Acín, *Efficient device-independent entanglement detection for multipartite systems*, Phys. Rev. X **7**, 021042 (2017).

[6] J. Bowles, I. Šupić, D. Cavalcanti, and A. Acín, *Device-independent entanglement certification of all entangled states*, Phys. Rev. Lett. **121**, 180503 (2018).

[7] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, *Bell nonlocality*, Rev. Mod. Phys. **86**, 419 (2014).

[8] I. Šupić and J. Bowles, *Self-testing of quantum systems: A review*, Quantum **4**, 337 (2020).

[9] F. Buscemi, *All entangled quantum states are nonlocal*, Phys. Rev. Lett. **108**, 200401 (2012).

[10] C. Branciard, D. Rosset, Y.-C. Liang, and N. Gisin, *Measurement-device-independent entanglement witnesses for all entangled quantum states*, Phys. Rev. Lett. **110**, 060405 (2013).

[11] M. Nawareg, S. Muhammad, E. Amselem, and M. Bourennane, *Experimental measurement-device-independent entanglement detection*, Sci. Rep. **5**, 8048 (2015).

[12] P. Xu, X. Yuan, L.-K. Chen, H. Lu, X.-C. Yao, X. Ma, Y.-A. Chen, and J.-W. Pan, *Implementation of a measurement-device-independent entanglement witness*, Phys. Rev. Lett. **112**, 140506 (2014).

[13] S. Kocsis, M. J. W. Hall, A. J. Bennet, D. J. Saunders, and G. J. Pryde, *Experimental measurement-device-independent verification of quantum steering*, Nat. Commun. **6**, 5886 (2015).

[14] Y. Guo, S. Cheng, X. Hu, B.-H. Liu, E.-M. Huang, Y.-F. Huang, C.-F. Li, G.-C. Guo, and E. G. Cavalcanti, *Experimental measurement-device-independent quantum steering and randomness generation beyond qubits*, Phys. Rev. Lett. **123**, 170402 (2019).

[15] Y.-Y. Zhao, H.-Y. Ku, S.-L. Chen, H.-B. Chen, F. Nori, G.-Y. Xiang, C.-F. Li, G.-C. Guo, and Y.-N. Chen, *Experimental demonstration of measurement-device-independent measure of quantum steering*, npj Quantum Inf. **6**, 77 (2020).

[16] M. F. Pusey, *Verifying the quantumness of a channel with an untrusted device*, J. Opt. Soc. Am. B **32**, A56 (2015).

[17] D. Rosset, F. Buscemi, and Y.-C. Liang, *Resource theory of quantum memories and their faithful verification with minimal assumptions*, Phys. Rev. X **8**, 021033 (2018).

[18] Y. Mao, Y.-Z. Zhen, H. Liu, M. Zou, Q.-J. Tang, S.-J. Zhang, J. Wang, H. Liang, W. Zhang, H. Li, L. You, Z. Wang, L. Li, N.-L. Liu, K. Chen, T.-Y. Chen, and J.-W. Pan, *Experimentally verified approach to nonentanglement-breaking channel certification*, Phys. Rev. Lett. **124**, 010502 (2020).

[19] F. Graffitti, A. Pickston, P. Barrow, M. Proietti, D. Kundys, D. Rosset, M. Ringbauer, and A. Fedrizzi, *Measurement-device-independent verification of quantum channels*, Phys. Rev. Lett. **124**, 010503 (2020).

[20] Y. Yu, P.-F. Sun, Y.-Z. Zhang, B. Bai, Y.-Q. Fang, X.-Y. Luo, Z.-Y. An, J. Li, J. Zhang, F. Xu, X.-H. Bao, and J.-W. Pan, *Measurement-device-independent verification of a quantum memory*, Phys. Rev. Lett. **127**, 160502 (2021).

[21] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, *High-rate measurement-device-independent quantum cryptography*, Nat. Photonics **9**, 397 (2015).

[22] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, *Gaussian quantum information*, Rev. Mod. Phys. **84**, 621 (2012).

[23] M. Tse, H. Yu, N. Kijbunchoo, A. Fernandez-Galiana, P. Dupej, L. Barsotti, C. Blair, D. Brown, S. Dwyer, A. Effler *et al.*, *Quantum-enhanced Advanced LIGO detectors in the era of gravitational-wave astronomy*, Phys. Rev. Lett. **123**, 231107 (2019).

[24] R. B. de Andrade, H. Kerdoncuff, K. Berg-Sørensen, T. Gehring, M. Lassen, and U. L. Andersen, *Quantum-enhanced continuous-wave stimulated raman scattering spectroscopy*, Optica **7**, 470 (2020).

[25] Y. Zhang, Y. Bian, Z. Li, S. Yu, and H. Guo, *Continuous-variable quantum key distribution system: Past, present, and future*, Appl. Phys. Rev. **11**, 011318 (2024).

[26] H.-S. Zhong, H. Wang, Y.-H. Deng, M.-C. Chen, L.-C. Peng, Y.-H. Luo, J. Qin, D. Wu, X. Ding, Y. Hu *et al.*, *Quantum computational advantage using photons*, Science **370**, 1460 (2020).

[27] L. S. Madsen, F. Laudenbach, M. F. Askarani, F. Rortais, T. Vincent, J. F. Bulmer, F. M. Miatto, L. Neuhaus, L. G. Helt, M. J. Collins *et al.*, *Quantum computational advantage with a programmable photonic processor*, Nature (London) **606**, 75 (2022).

[28] P. Abiuso, S. Bäuml, D. Cavalcanti, and A. Acín, *Measurement-device-independent entanglement detection for continuous-variable systems*, Phys. Rev. Lett. **126**, 190502 (2021).

[29] P. Abiuso, *Verification of continuous-variable quantum memories*, Quantum Sci. Technol. **9**, 01LT02 (2023).

[30] L.-M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, *Inseparability criterion for continuous variable systems*, Phys. Rev. Lett. **84**, 2722 (2000).

[31] R. Simon, *Peres-Horodecki separability criterion for continuous variable systems*, Phys. Rev. Lett. **84**, 2726 (2000).

[32] M. Horodecki, P. W. Shor, and M. B. Ruskai, *Entanglement breaking channels*, Rev. Math. Phys. **15**, 629 (2003).

[33] That is, entanglement breaking (EB) channels are of the form [32] $\Lambda^{\mathrm{EB}}[\rho] = \sum_a \rho^{(a)}\mathrm{Tr}[M^a\rho]$, where M^a represents a measurement operator with outcome a, and $\rho^{(a)}$ the corresponding quantum state prepared. It follows that an entanglement breaking memory (transmission line) would only need to store (send) the classical data a in order to simulate Λ at arbitrary distance in time (space).

[34] H. Yuen and M. Lax, *Multiple-parameter quantum estimation and measurement of nonselfadjoint observables*, IEEE Trans. Inf. Theory **19**, 740 (1973).

[35] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (Springer Science & Business Media, New York, 2011), Vol. 1.

[36] 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).

[37] S. L. Braunstein, C. A. Fuchs, and H. J. Kimble, *Criteria for continuous-variable quantum teleportation*, J. Mod. Opt. **47**, 267 (2000).

[38] D. Cavalcanti, P. Skrzypczyk, and I. Šupić, *All entangled states can demonstrate nonclassical teleportation*, Phys. Rev. Lett. **119**, 110501 (2017).

[39] While the verification procedure does not rely on trusting the measurement device, the calibration of the coherent states does require a trusted measurement device. This is a limitation of measurement-device-independent protocols compared to fully device independent protocols. However, MDI protocols can still be useful as the calibration of the coherent state generation can be performed in a trusted setting and subsequently used in untrusted settings.

[40] A. Verma, O. Solodovnikova, J. S. Neergaard-Nielsen, and U. L. Andersen, *Detecting non-Gaussian entanglement beyond Gaussian criteria*, arXiv:2512.17681.

[41] The causal separation can be taken as a reasonable experimental assumption, or it can be guaranteed via the requirement of the local measurements being space-like separated.

[42] L. Neuhaus, M. Croquette, R. Metzdorff, S. Chua, P.-E. Jacquet, A. Journeaux, A. Heidmann, T. Briant, T. Jacqmin, P.-F. Cohadon, and S. Deléglise, *Python Red Pitaya Lockbox (PYRPL): An open source software package for digital feedback control in quantum optics experiments*, Rev. Sci. Instrum. **95**, 033003 (2024).

[43] R. W. Drever, J. L. Hall, F. V. Kowalski, J. Hough, G. Ford, A. Munley, and H. Ward, *Laser phase and frequency stabilization using an optical resonator*, Appl. Phys. B **31**, 97 (1983).

[44] A. A. Hajomer, U. L. Andersen, and T. Gehring, *High-rate continuous-variable measurement device-independent quantum key distribution with finite-size security*, arXiv:2303.01611.

[45] R. Demkowicz-Dobrzański, M. Jarzyna, and J. Kołodyński, *Quantum limits in optical interferometry*, Prog. Opt. **60**, 345 (2015).

[46] S. Morelli, A. Usui, E. Agudelo, and N. Friis, *Bayesian parameter estimation using Gaussian states and measurements*, Quantum Sci. Technol. **6**, 025018 (2021).

[47] C. M. Caves, C. A. Fuchs, and R. Schack, *Unknown quantum states: The quantum de Finetti representation*, J. Math. Phys. (N.Y.) **43**, 4537 (2002).

[48] R. Renner and J. I. Cirac, *de finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography*, Phys. Rev. Lett. **102**, 110504 (2009).

[49] A. Leverrier, *Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction*, Phys. Rev. Lett. **118**, 200501 (2017).

[50] F. Dupuis, O. Fawzi, and R. Renner, *Entropy accumulation*, Commun. Math. Phys. **379**, 867 (2020).

[51] T. Metger, O. Fawzi, D. Sutter, and R. Renner, *Generalised entropy accumulation*, Commun. Math. Phys. **405**, 261 (2024)..

[52] A. E. Domínguez, W. E. O. Larcher, and C. N. Kozameh, *Fundamental residual amplitude modulation in electro-optic modulators*, arXiv:1710.10719.

[53] I. Suleiman, J. A. H. Nielsen, X. Guo, N. Jain, J. Neergaard-Nielsen, T. Gehring, and U. L. Andersen, *40 km fiber transmission of squeezed light measured with a real local oscillator*, Quantum Sci. Technol. **7**, 045003 (2022).