nature COMMUNICATIONS

ARTICLE

Received 25 Dec 2014 | Accepted 27 Aug 2015 | Published 18 Nov 2015

DOI: 10.1038/ncomms9498 OPEN

Reliable quantum certification of photonic state preparations

Leandro Aolita[1,2], Christian Gogolin[1,3,4], Martin Kliesch[1] & Jens Eisert[1]

Quantum technologies promise a variety of exciting applications. Even though impressive progress has been achieved recently, a major bottleneck currently is the lack of practical certification techniques. The challenge consists of ensuring that classically intractable quantum devices perform as expected. Here we present an experimentally friendly and reliable certification tool for photonic quantum technologies: an efficient certification test for experimental preparations of multimode pure Gaussian states, pure non-Gaussian states generated by linear-optical circuits with Fock-basis states of constant boson number as inputs, and pure states generated from the latter class by post-selecting with Fock-basis measurements on ancillary modes. Only classical computing capabilities and homodyne or hetorodyne detection are required. Minimal assumptions are made on the noise or experimental capabilities of the preparation. The method constitutes a step forward in many-body quantum certification, which is ultimately about testing quantum mechanics at large scales.

[1] Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany. [2] Instituto de Física, Universidade Federal do Rio de Janeiro, P. O. Box 68528, Rio de Janeiro 21941-972, Brazil. [3] ICFO-Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels (Barcelona), Spain. [4] Max-Planck-Institut für Quantenoptik, Hans-Kopfermann-Str. 1, 85748 Garching, Germany. Correspondence and requests for materials should be addressed to J.E. (email: jenseisert@gmail.com).

Many-body quantum devices promise exciting applications in ultraprecise quantum metrology[1], quantum computing[2–4] and quantum simulators[5–9]. In the quest for their large-scale realization, impressive progress on a variety of quantum technologies has recently been made[6–9]. Among these technologies, optical platforms play a key role. For example, sophisticated manipulations of multi-qubit entangled states of up to eight parametrically downconverted photons[10,11] have been demonstrated and continuous-variable entanglement among 60 stable[12] and up to 10,000 flying[13] modes has been verified in optical set-ups. In addition, small-sized simulations of BosonSampling[14–17] and Anderson localization in quantum walks[18,19] have been performed with on-chip integrated linear-optical networks.

This fast pace of advance, however, makes the problem of reliable certification an increasingly pressing issue[20–24]. From a practical viewpoint, further experimental progress on many-body quantum technologies is nowadays hindered by the lack of practical certification tools. At a fundamental level, certifying many-body quantum devices is ultimately about testing quantum mechanics in regimes where it has never been tested before.

Tomographic characterization of quantum states requires the measurement of exponentially many observables. Compressed-sensing techniques[25] reduce, for states approximated by low-rank density matrices, the requirements significantly, but still demand exponentially many measurements. Efficient certification techniques, requiring only polynomially many measurements, for universal quantum computation[26–28] and a restricted model of computation with one pure qubit[29] exist in the form of quantum interactive proofs. However, these require either a fully fledged fault-tolerant universal quantum computer[26–28] or an experimentally non-trivial measurement-based quantum device[29]. In addition, these methods involve sequential interaction rounds with the device[26–29]. In contrast, permutationally invariant tomography[30], tensor network techniques[31], Monte Carlo fidelity estimation[32–34], and Clifford-circuit benchmarking techniques[35] provide experimentally friendly alternatives for the efficient certification of preparations of permutationally invariant[30] and qubit stabilizer or W states[32–35], respectively. Nevertheless, none of these methods addresses continuous-variable systems, not even in Gaussian states.

Here we introduce an experimentally friendly technique for the certification of continuous-variable state preparations without estimating the prepared state itself. First, we discuss intuitively and define precisely reliable quantum-state certification tests. We do this for two notions of certification, differing in that in one of them robustness against small preparation errors is mandatory. Then, we present a certification test, based on single-mode homodyne and heterodyne detection, for arbitrary m-mode pure Gaussian states, pure non-Gaussian states resulting from passive Gaussian unitary operations on Fock-basis states with n photons, and pure states prepared by post-selecting states in the latter class with Fock-basis measurements on $a<m$ ancillary modes. This covers, for instance, Gaussian quantum simulations such as those of refs 12,13 as well as the non-Gaussian ones of refs. 6,10,11,14–19. Furthermore, both photon-added or -subtracted linear-optical network states[36–39] as well as all non-Gaussian states accessible to qumode-encoded qubit[40,41] quantum computers also lie within the range of applicability of our method. For all Gaussian states and all mentioned non-Gaussian states with constant n, the protocol is efficient in m and, for the cases with post-selection, also in the inverse post-selection success probability.

With high probability, our test rejects all experimental preparations with a fidelity with respect to the chosen target state lower than a desired threshold and accepts if the preparation is sufficiently close to the target. That is, the protocol is robust against small preparation errors. We upper-bound the failure probability in terms of the number of experimental runs and calculate the necessary number of measurement settings. Our method is built on a fidelity lower bound, based on a natural extremality property, that is interesting in its own right. Finally, the experimental estimation of this bound relies on non-Gaussian state nullifiers, which we introduce on the way.

Results

Certification notions. We present our results in terms of photons propagating through optical networks, but our methods apply to any bosonic platform with equivalent dynamics. We consider a sceptic certifier, Arthur, with limited quantum capabilities, who wishes to ascertain whether an untrusted quantum prover, Merlin, presumably with more quantum capabilities, can indeed prepare certain quantum states that Arthur cannot. This mindset is reminiscent to that of quantum interactive-proof systems[26–29] of computer science, but our method has the advantage that no interaction apart from the measurements of the certifier on the single-run experimental preparations from the prover is required.

In particular, we consider the situation where Merlin possesses at least a network of active single-mode squeezers and displacers as well as passive beam-splitters and phase-shifters, sufficient to efficiently implement any m-mode Gaussian unitary[42–46], plus single-photon sources. Arthur's resources, in contrast, are restricted to classical computational power augmented with single-mode measurements. With that, he can characterize each of his single-mode measurement channels up to any desired constant precision. The task is for Merlin to provide Arthur with copies of an m-mode pure target state ϱ_t of Arthur's choice. We assume that Merlin follows independent and identical state-preparation procedures on each experimental run, described by the density matrix ϱ_p. We refer to ϱ_p as a preparation of the target state ϱ_t. His preparation is unavoidably subject to imperfections and he might even be dishonest and try to trick Arthur. Thus, Arthur would like to run a test, with his own measurement devices, to certify whether ϱ_p is indeed a *bona fide* preparation of ϱ_t.

To measure how good a preparation ϱ_p of ϱ_t is, we use the fidelity between ϱ_p and ϱ_t, which we define as

$$F := F\left(\varrho_t, \varrho_p\right) := \mathrm{Tr}\left[\left(\sqrt{\varrho_t}\varrho_p^{\dagger}\sqrt{\varrho_t}\right)^{1/2}\right]^2 = \mathrm{Tr}\left[\varrho_t\varrho_p\right], \quad (1)$$

where the last equality holds because ϱ_t is assumed to be pure. Another usual definition of the fidelity corresponds to the square root of the fidelity as defined above. All our results can be adapted to that definition and also to the trace distance $D := D(\varrho_t, \varrho_p)$, which can be defined via the 1-norm distance in state space as $D(\varrho_t,\varrho_p) := \mathrm{Tr}[|\varrho_t - \varrho_p|]/2$. Note that D can be bounded from both sides in terms of F, as defined in equation (1), through the well-known inequalities $1-F \leq D \leq \sqrt{1-F}$, where the first inequality holds because ϱ_t is pure.

Let us first discuss what properties an experimental test must fulfil to qualify as a state certification protocol. Different certification paradigms are schematically represented in Fig. 1. We start with the formal definition of certification in the sense of Fig. 1c.

Definition 1 (Quantum-state certification). Let ϱ_t be a target state, $F_T<1$ a threshold fidelity, and $\alpha>0$ a maximal failure probability. A test, which takes as input copies of a preparation ϱ_p and outputs 'accept' or 'reject', is a certification test for ϱ_t if, with probability at least $1-\alpha$, it both rejects every ϱ_p for which

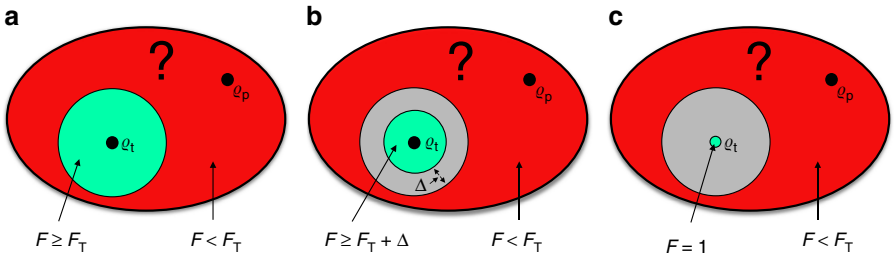

Figure 1 | Different certification paradigms. (**a**) Naive approach: To certify an untrusted experimental preparation ϱ_p of the target state ϱ_t, a certifier Arthur would like to run a statistical test that, for all ϱ_p, decides whether the fidelity F between ϱ_p and ϱ_t is greater or equal than a prespecified threshold $F_T<1$ (inner green region, accept), or smaller than it (outer red region, reject). However, due to the preparations at the boundary of the two regions and experimental uncertainties, a test able to make such a decision does not exist. (**b**) The ideal scenario: A more realistic certification notion is to ask that the test rejects every ϱ_p for which $F<F_T$ (outer red region) and accepts every ϱ_p for which $F\geq F_T+\Delta$ (inner green region), for some given $\Delta<1-F_T$. Here a buffer region of width Δ (in grey) is introduced within which the behaviour of the test can be arbitrary, but, in return, the certification is now feasible. This type of certification is thus robust against experimental infidelities as large as $1-F_T-\Delta$. (**c**) The practical scenario: Finally, the least one can demand is that the test rejects every ϱ_p for which $F<F_T$ (outer red region) and accepts at least ϱ_t (green point). The former condition is sometimes called soundness and the latter one completeness. Here no acceptance is guaranteed for any ϱ_p with $F\geq F_T$ (grey region) other than ϱ_t itself, but any ϱ_p accepted by the test necessarily features $F\geq F_T$. This certification notion is not necessarily robust against state deviations, but it can be more practical. In addition, in practice, the resulting tests succeed also in accepting many $\varrho_p\neq\varrho_t$ for which $F\geq F_T$.

$F(\varrho_t,\varrho_p) < F_T$ and accepts if $\varrho_p=\varrho_t$. We say that any ϱ_p accepted by such a test is a certified preparation of ϱ_t.

Classes of target states. To specify the target states we need to introduce some notation. We denote m-mode Fock basis states by $|n\rangle$, with $\mathbf{n}:=(n_1, n_2,\ldots,n_m)$ being the sequence of photon numbers $n_j\geq 0$ in each mode $j\in[m]$, where the short-hand notation $[m]:=\{1, 2,\ldots,m\}$ is introduced, and call $n:=\sum_{j=1}^m n_j$ the total input photon number. In particular, we will pay special attention to Fock basis states $|\mathbf{1}_n\rangle$ with exactly one photon in each of the first n modes and the vacuum in the remaining $m-n$ ones, that is, those for which $\mathbf{n}=\mathbf{1}_n$, with

$$\mathbf{1}_n := (\underbrace{1,\ldots,1}_{n\text{ times}},\underbrace{0,\ldots,0}_{m-n\text{ times}}) \tag{2}$$

Note that $|\mathbf{1}_0\rangle$ is the Gaussian vacuum state $|\mathbf{0}\rangle$. We denote the photon number operator corresponding to mode j by $\hat{n}_j$ and the total photon number operator by $\hat{n}:=\sum_{j=1}^m \hat{n}_j$.

In addition, for post-selected target states, we denote by $\mathcal{A}:=\{\mathcal{A}_j\}_{j\in[a]}$, where each element $\mathcal{A}_j\in[m]$ labels a different mode, the subset of $a:=|\mathcal{A}|<m$ modes on which the post-selection measurements are made. We then identify the remaining $m-a$ modes as the system subset $\mathcal{S}$, which carries the post-selected target state $\varrho_{\mathcal{S}_t}$. The subindex $\mathcal{S}$ emphasizes that $\varrho_{\mathcal{S}_t}$ represents an $(m-a)$-mode post-selected target state and distinguishes it from m-mode target states without post-selection, which we denote simply as ϱ_t. We denote by $|\mathbf{n}_\mathcal{A}\rangle_\mathcal{A}$, with $\mathbf{n}_\mathcal{A}:=(n_{\mathcal{A}_1}, n_{\mathcal{A}_2},\ldots, n_{\mathcal{A}_a})$, an a-mode pure normalized Fock-basis state of $n_\mathcal{A}:=\sum_{j=1}^a n_{\mathcal{A}_j}$ total photons on the modes $\mathcal{A}$. We use the short-hand notations $\langle\mathbf{n}_\mathcal{A}|_\mathcal{A}\varrho_t|\mathbf{n}_\mathcal{A}\rangle_\mathcal{A}:=\mathrm{Tr}_\mathcal{A}\left[\varrho_t(\mathbb{1}_\mathcal{S}\otimes|\mathbf{n}_\mathcal{A}\rangle_\mathcal{A}\langle\mathbf{n}_\mathcal{A}|_\mathcal{A})\right]$, where $\mathrm{Tr}_\mathcal{A}$ indicates partial trace over the Fock space of $\mathcal{A}$, $\mathbb{1}_\mathcal{S}$ denotes the identity on $\mathcal{S}$, and $\mathbb{P}(\mathbf{n}_\mathcal{A}|\varrho_t):=\mathrm{Tr}\left[\langle\mathbf{n}_\mathcal{A}|_\mathcal{A}\varrho_t|\mathbf{n}_\mathcal{A}\rangle_\mathcal{A}\right]$ is the post-selection success probability, that is, the probability of measuring $|\mathbf{n}_\mathcal{A}\rangle_\mathcal{A}$ in a projective measurement on $\mathcal{A}$. Without loss of generality, we consider throughout only the non-trivial case $\mathbb{P}(\mathbf{n}_\mathcal{A}|\varrho_t)\neq 0$.

With the notation introduced, we derive our results for: arbitrary m-mode pure Gaussian states, given by the class

$$\mathcal{C}_\mathrm{G} := \left\{\varrho_t=\hat{U}|\mathbf{0}\rangle\langle\mathbf{0}|\hat{U}^\dagger : \hat{U}\text{ Gaussian unitary}\right\}, \tag{3}$$

m-mode pure linear-optical network states from the class

$$\mathcal{C}_\mathrm{LO} := \left\{\varrho_t=\hat{U}|\mathbf{1}_n\rangle\langle\mathbf{1}_n|\hat{U}^\dagger : \hat{U}\text{ passive unitary}\right\}, \tag{4}$$

and $(m-a)$-mode pure locally post-selected linear-optical network states from the class

$$\mathcal{C}_\mathrm{PLO} := \left\{\varrho_{\mathcal{S}_t}:=\frac{\langle\mathbf{n}_\mathcal{A}|_\mathcal{A}\varrho_t|\mathbf{n}_\mathcal{A}\rangle_\mathcal{A}}{\mathbb{P}(\mathbf{n}_\mathcal{A}|\varrho_t)} : \varrho_t\in\mathcal{C}_\mathrm{LO}\right\}. \tag{5}$$

The three classes of target states are schematically represented in Fig. 2. The class $\mathcal{C}_\mathrm{G}$ is crucial within the realm of 'continuous-variable' quantum optics and quantum information processing. It encompasses, for instance, 'twin-beam' (two-mode squeezed vacuum) states under passive networks, which are used to simulate, upon coincidence detection, multi-qubit states[6]. The class $\mathcal{C}_\mathrm{LO}$ includes all the settings sometimes referred to as 'discrete variable' linear-optical networks. This class covers, among others, the targets of several recent experimental simulations with on-chip integrated linear-optical networks[14–19]. The third class, $\mathcal{C}_\mathrm{PLO}$, is the one of linear-optical network states locally post-selected with Fock-basis measurements. This class includes important non-Gaussian resources for quantum information and quantum optics. For instance, it encompasses both photon-added or -subtracted linear-optical network states[36–39]. Furthermore, when n is proportional to m, it also includes all the states prepared by probabilistic schemes of the type of refs 40,41 for universal qumode-encoded qubit quantum computation.

The certification test. The basis of the our certification scheme is a technique for the estimation of the quantity

$$F^{(n)} := \left\langle (n+1-\hat{n})\prod_{j=1}^n \hat{n}_j \right\rangle_{\hat{U}^\dagger\varrho_p\hat{U}}, \tag{6}$$

with n the total input photon number. As shown in the Methods section, for all target states $\varrho_t\in\mathcal{C}_\mathrm{G}\cup\mathcal{C}_\mathrm{LO}$, $F^{(n)}$ is a lower bound on the fidelity F and, moreover, $F^{(n)}=F=1$ if $\varrho_p=\varrho_t$. In addition, this bound is connected to a natural extremality property of Gaussian states, discussed also in the Methods section. Our test $\mathcal{T}$, summarized in Box 1, yields an estimate $F^{(n)^*}$ of $F^{(n)}$. If $F^{(n)^*}$ is sufficiently above the threshold F_T, the preparation ϱ_p is accepted. Otherwise it is rejected. We introduce the measurement schemes $\mathcal{M}_\mathrm{G}$ and $\mathcal{M}_\mathrm{LO}$, which depend on the

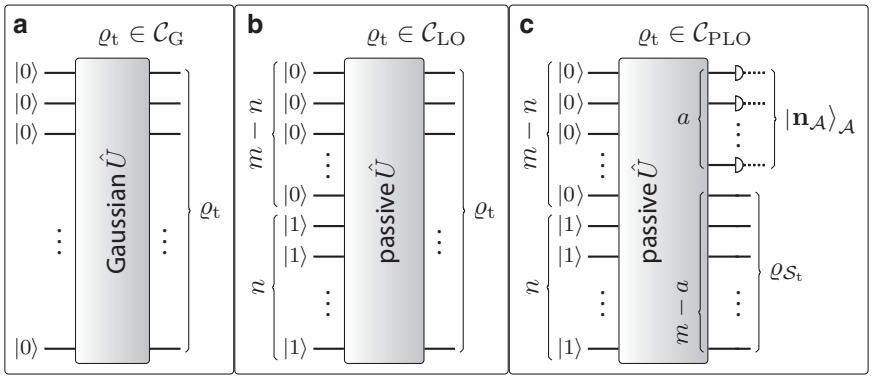

Figure 2 | Classes of target states. (**a**) $\mathcal{C}_G$ is the class composed of all m-mode pure Gaussian states. These can be prepared by applying an arbitrary Gaussian unitary $\hat{U}$ (possibly involving multimode squeezing) to the m-mode vacuum state $|\mathbf{0}\rangle$. (**b**) The class $\mathcal{C}_{LO}$ includes all m-mode pure non-Gaussian states produced at the output of an arbitrary linear-optical network, which implements a passive Gaussian unitary $\hat{U}$ (without squeezing), with the Fock-basis state $|\mathbf{1}_n\rangle$ containing one photon in each of the first n modes and zero in the remaining $m-n$ ones as input. As the order of the modes is arbitrary, choosing the first n modes as the populated ones does not constitute a restriction. (**c**) The third class, $\mathcal{C}_{PLO}$ encompasses all $(m-a)$-mode pure non-Gaussian states obtained by projecting a subset $\mathcal{A}$ of $a<m$ modes of an m-mode pure linear-optical network state $\varrho_t \in \mathcal{C}_{LO}$ onto a pure normalized product Fock-basis state $|\mathbf{n}_\mathcal{A}\rangle_\mathcal{A}$. In practice, this is done probabilistically by measuring $\mathcal{A}$ in a local basis that contains $|\mathbf{n}_\mathcal{A}\rangle_\mathcal{A}$ and post-selecting only the events in which $|\mathbf{n}_\mathcal{A}\rangle_\mathcal{A}$ is measured. Thus, the a modes in $\mathcal{A}$ are used as ancillas, whereas the effective system is given by the subset $\mathcal{S}$ containing the other $m-a$ modes, which carries the final target state. For concreteness, but without any loss of generality, in the plot, the ancillary modes are chosen to be the last a ones. These three classes cover the target states considered in the vast majority of quantum photonic experiments.

Box 1 | (Certification test $\mathcal{T}$).

Settings adjustments: Arthur chooses a threshold fidelity $F_T<1$, a maximal failure probability $\alpha>0$, and an estimation error $0<\varepsilon\leq(1-F_T)/2$.

State request: Arthur provides Merlin with the classical specification n, $\mathbf{S}$ and $\mathbf{x}$ of the target state ϱ_t and requests a sufficient number of copies of it.

Quantum measurements: If $n=0$, Arthur measures $2m\kappa$ two-mode correlations and $2m$ single-mode expectation values specified by the measurement scheme $\mathscr{M}_G$ (see the Methods section), which can be done with $m+3$ local homodyne settings or a single local heterodyne setting throughout.

If $n>0$, he measures $O(m(4d^2+1)^n)$ multi-body correlators, each one involving between 1 and $2n+1$ modes, specified by the measurement scheme $\mathscr{M}_{LO}$ (see the Methods section), which can be done with a single local heterodyne setting throughout.

Classical post-processing: By processing the measurement outcomes (see the Methods section), he obtains a fidelity estimate $F^{(n)\star}$ such that $F^{(n)\star}\in[F^{(n)}-\varepsilon, F^{(n)}+\varepsilon]$ with probability at least $1-\alpha$, where $F^{(n)}$ is the lower bound to F given by expression (6).

Accept-reject decision: If $F^{(n)\star}<F_T+\varepsilon$, he rejects. Otherwise, he accepts.

specific target state, to obtain the estimate $F^{(n)\star}$. Gaussian states can be estimated with the scheme $\mathcal{M}_G$, while linear-optical network states with $\mathcal{M}_{LO}$. Both measurement schemes are summarized in the Methods section and described in detail in Supplementary Note 1. In turn, a fidelity bound for post-selected target states in $\mathcal{C}_{PLO}$ similar to $F^{(n)}$ is presented in the Methods section. Its derivation, the adaptation of the test $\mathcal{T}$ to post-selected targets, and the corresponding measurement scheme are provided in Supplementary Note 2.

Our theorems guarantee that the test from Box 1 is indeed a certification test and give a bound on the scaling of the number of samples that are needed for the test. To state them, we introduce some notation related to mode space descriptions of linear-optical networks first. Any Gaussian unitary transformation $\hat{U}$ on Hilbert space can be represented by an affine symplectic transformation in mode space, that is, by a symplectic matrix $\mathbf{S}\in\mathrm{Sp}(2m,\mathbb{R})$ followed by a phase-space displacement $\mathbf{x}\in\mathbb{R}^{2m}$ (see equation (25) in the Methods section), where the real-symplectic group $\mathrm{Sp}(2m,\mathbb{R})$ contains all real $2m\times 2m$ matrices that preserve the canonical phase-space commutation relations[42,43]. By virtue of the Euler decomposition[42,45], $\mathbf{S}$ can be implemented with single-mode squeezing operations and passive mode transformations. We denote the maximum single-mode squeezing of $\mathbf{S}$ by s_{max} and define the mode range $d\leq m$ to be the maximal number of input modes to which each output mode is coupled (for details see Supplementary Note 1). Also, it will be useful to define

$$\kappa := 2\min\{d^2, m\}. \tag{7}$$

The displacement $\mathbf{x}$ can be implemented by a single-mode displacer at each mode $j\in[m]$, with amplitude (x_{2j-1}, x_{2j}), where x_k, for $k\in[2m]$, is the kth component of $\mathbf{x}$. The vector 2-norm is denoted by $\|\cdot\|_2$, that is, $\|\mathbf{x}\|_2:=\left(\sum_{k=1}^{2m}x_k^2\right)^{1/2}$.

We take σ_i to be a uniform upper bound on the variances of any product of i phase-space quadratures in the state ϱ_p. If ϱ_p is Gaussian, then σ_1 and σ_2 are functions of the single-mode squeezing parameters of ϱ_p. In addition, we call $\sigma_{\leq i}:=\max_{k\leq i}\{\sigma_k\}$ the maximal ith variance of ϱ_p. Finally, we use the Landau symbol O to denote asymptotic upper bounds.

Theorem 2 (Quantum certification of Gaussian states). Let $F_T<1$ be a threshold fidelity, $\alpha>0$ a maximal failure probability, and $0<\varepsilon\leq(1-F_T)/2$ an estimation error. Let $\varrho_t\in\mathcal{C}_G$ have maximum single-mode squeezing $s_{max}\geq 1$, mode range $d\leq m$, and displacement $\mathbf{x}$. Test $\mathcal{T}$ from Box 1 is a certification test for ϱ_t and requires at most

$$O\left(\frac{s_{max}^4\left(2\sigma_1^2\|\mathbf{x}\|_2^2m^3+\sigma_2^2\kappa^3m^4\right)}{\varepsilon^2\ln(1/(1-\alpha))}\right) \tag{8}$$

copies of a preparation ϱ_p with first and second variance bounds $\sigma_1>0$ and $\sigma_2>0$, respectively.

Theorem 3 (Quantum certification of linear-optical network states). Let $F_T<1$ be a threshold fidelity, $\alpha>0$ a maximal failure

probability, and $0<\varepsilon\leq(1-F_{\mathrm{T}})/2$ an estimation error. Let $\varrho_{\mathrm{t}}\in\mathcal{C}_{\mathrm{LO}}$ have mode range $d\leq m$. Test $\mathcal{T}$ from Box 1 is a certification test for ϱ_{t} and requires at most

$$\mathrm{O}\left(\frac{\sigma^2_{\leq 2(n+1)}m^4(\lambda d^6\, n\, m)^n}{\varepsilon^2\ln(1/(1-\alpha))}\right) \tag{9}$$

copies of a preparation ϱ_{p} with maximal $2(n+1)$-th variance $\sigma_{\leq 2(n+1)}$, where $\lambda>0$ is an absolute constant.

The proofs of all our theorems are provided in the Supplementary Information. The treatment of the class $\mathcal{C}_{\mathrm{PLO}}$ follows as a corollary of Theorem 3 and is also provided in Supplementary Note 2. Equations (8) and (9) are highly simplified upper bounds on the total number of copies of ϱ_{p} that $\mathcal{T}$ requires. For more precise expressions see Supplementary Lemmas 6 and 9. Note that neither of the two theorems requires any energy cut-off or phase-space truncation. While the bound in equation (9) is inefficient in n, both for the Gaussian and linear-optical cases, the number of copies of ϱ_{p} scales polynomially with all other parameters, in particular with m. Thus, arbitrary m-mode target states from the classes $\mathcal{C}_{\mathrm{G}}$ and $\mathcal{C}_{\mathrm{LO}}$ with constant n, are certified by $\mathcal{T}$ efficiently.

Interestingly, since states in $\mathcal{C}_{\mathrm{LO}}$ in general display negative Wigner functions, sampling from their measurement probability distributions cannot be efficiently done by the available classical sampling methods[47–49]. Furthermore, for Fock-state measurements, these distributions define BosonSampling, for which hardness results exist[50] for m asymptotically lower bounded by n^5.

Also, note that there are no restrictions on ϱ_{p} except that, in practice, to apply the theorems, one needs bounds on σ_1, σ_2, and $\sigma_{\leq 2(n+1)}$. These variances are properties of ϱ_{p} and are therefore *a priori* unknown to Arthur. However, he can reasonably estimate them from his measurements. Note that, for random variables that can take any real value, assuming that the variances are bounded is a fundamental and unavoidable assumption to make estimations from samples; and it is one that can be contrasted with the measurement results.

Robustness against preparation imperfections. To end up with, we consider certification in the sense of Fig. 1b:

Definition 4 (Robust quantum-state certification). Let ϱ_{t} be a target state, $F_{\mathrm{T}}<1$ be a threshold fidelity, $\alpha>0$ a maximal failure probability, and $\Delta<1-F_{\mathrm{T}}$ a fidelity gap. A test, which takes as input copies of a preparation ϱ_{p} and outputs 'accept' or 'reject', is a robust certification test for ϱ_{t} if, with probability at least $1-\alpha$, it both rejects every ϱ_{p} for which $F(\varrho_{\mathrm{t}},\varrho_{\mathrm{p}})<F_{\mathrm{T}}$ and accepts every ϱ_{p} for which $F(\varrho_{\mathrm{t}},\varrho_{\mathrm{p}})\geq F_{\mathrm{T}}+\Delta$. We say that any ϱ_{p} accepted by such a test is a certified preparation of ϱ_{t}.

This definition is more stringent than Definition 1 in that it guarantees that preparations sufficiently close to ϱ_{t} are necessarily accepted, rendering the certification robust against preparation imperfections causing fidelity deviations as large as $1-(F_{\mathrm{T}}+\Delta)$. We now show that our test $\mathcal{T}$ from Box 1 is actually a robust certification test.

To this end, we first write ϱ_{p} as

$$\varrho_{\mathrm{p}}=F\varrho_{\mathrm{t}}+(1-F)\varrho_{\mathrm{t}}^{\perp}, \tag{10}$$

where $\varrho_{\mathrm{t}}^{\perp}$ is an operator orthogonal to ϱ_{t} with respect to the Hilbert–Schmidt inner product, that is, such that $\mathrm{Tr}\left[\varrho_{\mathrm{t}}\varrho_{\mathrm{t}}^{\perp}\right]=0$. As ϱ_{t} is assumed to be pure, it follows immediately that $\varrho_{\mathrm{t}}^{\perp}$ is actually a state. In fact, multiplying both sides of equation (10) by ϱ_{t} and taking the trace, one readily sees that decomposition in equation (10) is just another way to express the fidelity in equation (1).

According to equation (6), the lower bound $F^{(n)}$ can be defined as an expectation value of the observable

$$\hat{F}^{(n)}:=\hat{U}\left((n+1-\hat{n})\prod_{j=1}^{n}\hat{n}_j\right)\hat{U}^{\dagger} \tag{11}$$

with respect to ϱ_{p}. In a similar way, we define the quantity

$$F_{\perp}^{(n)}:=\left\langle\hat{F}^{(n)}\right\rangle_{\varrho_{\mathrm{t}}^{\perp}}. \tag{12}$$

By taking the expectation value of equation (10) with respect to the observable $\hat{F}^{(n)}$ and using that $\mathrm{Tr}\left[\hat{F}^{(n)}\varrho_{\mathrm{t}}\right]=1$ and $F^{(n)}\leq F$, one finds that $F_{\perp}^{(n)}\leq 0$. The parameter $F_{\perp}^{(n)}$ turns out to quantify the robustness of our certification test.

Theorem 5 (Robust quantum certification). Under the same conditions as in Theorems 2 and 3, test $\mathcal{T}$ from Box 1 is a robust certification test with fidelity gap

$$\Delta:=\frac{2\varepsilon+F_{\perp}^{(n)}(F_{\mathrm{T}}-1)}{1-F_{\perp}^{(n)}}. \tag{13}$$

Since $F_{\perp}^{(n)}\leq 0$ and $F_{\mathrm{T}}<1$, it is clear that $\Delta>0$. On the other hand, note that $F_{\perp}^{(n)}$ can in general be arbitrarily smaller than zero. This happens, for instance, for preparations for which $\hat{U}^{\dagger}\varrho_{\mathrm{t}}^{\perp}\hat{U}=|\mathbf{n}\rangle\langle\mathbf{n}|$, with $n_1, n_2,\ldots,n_n\geq 1$ and n arbitrarily large. In particular, in the limit $F_{\perp}^{(n)}\to-\infty$, it holds that $\Delta\to 1-F_{\mathrm{T}}$, so that the certification becomes less robust with decreasing $F_{\perp}^{(n)}$, as one would expect. In contrast, as $F_{\perp}^{(n)}$ increases from $-\infty$ to 0, the gap decreases to its minimal value $\Delta=2\varepsilon$. Note that, since it depends on $\varrho_{\mathrm{t}}^{\perp}$, $F_{\perp}^{(n)}$ cannot be directly estimated from measurements on ϱ_{p} alone. However, Theorem 5 guarantees the existence of an entire closed convex set of states around ϱ_{t} that are rightfully accepted and Δ lower bounds the size of that region. Furthermore, in experimentally relevant situations, $\left|F_{\perp}^{(n)}\right|$ is expected to be small, meaning that Δ is close to its optimal value 2ε.

Finally, a statement equivalent to Theorem 5 for target states $\varrho_{\mathcal{S}_{\mathrm{t}}}\in\mathcal{C}_{\mathrm{PLO}}$ follows as an immediate corollary of it and is Supplementary Note 2.

Discussion

Large-scale photonic quantum technologies promise important scientific advances and technological applications. So far, considerably more effort has been put into their realization than into the verification of their correct functioning and reliability. This imposes a serious obstacle for further experimental advance, specifically in the light of the speed at which progress towards many-mode architectures takes place. Here we have presented a practical reliable certification tool for a broad family of multimode bosonic quantum technologies.

We have proven theorems that upper bound the number of experimental runs sufficient for our protocol to be a certification test. Our theorems provide large-deviation bounds from a simple extremality-based fidelity lower bound that is interesting in its own right. Our theorems hold only for statistical errors, but the stability analysis on which they rely (see Supplementary Lemmas 5 and 8) holds regardless of the nature of the errors. In Supplementary Note 5, we show that our fidelity estimates are robust also against small systematic errors.

From a more practical viewpoint, our test allows one to certify the state preparations of most current optical experiments, in both the 'continuous-variable' and the 'discrete-variable' settings. This is achieved under the minimal possible assumptions: namely, only that the variances of the measurement outcomes

are finite. Thus, the certification is as unconditional as the fundamental laws of statistics allow. In particular, no assumption on the type of noise is made. Despite the rigorous bounds on the estimation errors and failure probabilities, our methods are both experimentally friendly and resource efficient.

Notably, our test can efficiently certify multimode negative-Wigner-function states that define, via local measurements, sampling problems whose classical simulation is not known to be efficient[47–49]. For instance, it can be applied to the certification of optical circuits of the type used in BosonSampling: There, m-mode Fock-basis states of n photons are subjected to a linear-optical network described by a random unitary $\hat{U}$ drawn from the Haar measure[50] and, subsequently, each output mode is measured in the Fock basis. While the question of the certification of the classical outcomes of such samplers without assumptions on the device is still largely open[20,21], with the methods described here the premeasurement non-Gaussian quantum outputs of BosonSampling devices[14–17] can be certified reliably and, for constant n, even efficiently. In this sense, this work goes significantly beyond previously proposed schemes to rule out particular cheating strategies by the prover[21–24]. Furthermore, a variety of non-Gaussian states paradigmatic in quantum optics and quantum information are also covered by our protocol (see Supplementary Note 2 for details). These include, for instance, linear-optical network outputs post-selected though photon-number measurements, ranging from both photon-added or -subtracted linear-optical network states[36–39] to all the states preparable with Knill–Laflamme–Milburn-like schemes[40,41]. For all such states, our test is efficient in the inverse post-selection success probability $1/\mathbb{P}(\mathbf{n}_{\mathcal{A}}|\varrho_{\mathrm{t}})$.

The present method constitutes a step forward in the field of photonic quantum certification, with potential implications on the certification of other many-body quantum-information technologies. Apart from that of BosonSamplers and optical schemes with post-selection, the efficient and reliable certification of large-scale photonic networks as those used, for instance, for multimode Gaussian quantum-information processing[12,13], non-Gaussian Anderson-localization simulations[18,19], and quantum metrology[1], with a constant number of input photons, is now within reach.

Methods

Fidelity lower bound. Here we formalize the extremality notion and derive a lower bound on the fidelity F for non post-selected target states. All the non post-selected target states we consider are of the form

$$\varrho_{\mathrm{t}} = \hat{U}|\mathbf{n}\rangle\langle\mathbf{n}|\hat{U}^{\dagger}, \tag{14}$$

where $\hat{U}$ is an arbitrary Gaussian unitary and $|\mathbf{n}\rangle$ an arbitrary Fock-basis state. First, we derive a fidelity lower bound for general states of the form given in equation (14) and then consider the linear-optical and Gaussian cases separately. Lower bounds for the post-selected target states are provided further below in the Measurement Scheme.

We start recalling that

$$|\mathbf{n}\rangle = \prod_{j=1}^{m} \frac{1}{\sqrt{n_j!}} \left(\hat{a}_j^{\dagger}\right)^{n_j} |\mathbf{0}\rangle, \tag{15}$$

where $a_j^{\dagger}$ is the creation operator of the jth mode. Its Hermitian conjugated $\hat{a}_j$ is the corresponding annihilation operator. These operators satisfy $\left[\hat{a}_j, \hat{a}_{j'}^{\dagger}\right] = \delta_{j,j'}$, where $\delta_{j,j'}$ denotes the Kronecker delta of j and j', and $\hat{n}_j = \hat{a}_j^{\dagger}\hat{a}_j$, for all $j, j' \in [m]$. The fidelity in equation (1) can be written as $F = F\left(|\mathbf{n}\rangle\langle\mathbf{n}|, \tilde{\varrho}_{\mathrm{p}}\right)$, where $\tilde{\varrho}_{\mathrm{p}} := \hat{U}^{\dagger}\varrho_{\mathrm{p}}\hat{U}$ is the Heisenberg representation of ϱ_{p} with respect to $\hat{U}^{\dagger}$. With this, equation (15), and the cyclicality property of the trace, we obtain that

$$F = \mathrm{Tr}\left[|\mathbf{0}\rangle\langle\mathbf{0}|\tilde{\varrho}_{\mathrm{p},\mathbf{n}}\right] = F\left(|\mathbf{0}\rangle\langle\mathbf{0}|, \tilde{\varrho}_{\mathrm{p},\mathbf{n}}\right), \tag{16}$$

where

$$\tilde{\varrho}_{\mathrm{p},\mathbf{n}} := \prod_{j'=1}^{m} \frac{1}{\sqrt{n_{j'}!}} \left(\hat{a}_{j'}\right)^{n_{j'}} \tilde{\varrho}_{\mathrm{p}} \prod_{j=1}^{m} \frac{1}{\sqrt{n_j!}} \left(\hat{a}_j^{\dagger}\right)^{n_j} \tag{17}$$

is a (not necessarily normalized) positive-semidefinite operator.

To lower bound $F\left(|\mathbf{0}\rangle\langle\mathbf{0}|, \tilde{\varrho}_{\mathrm{p},\mathbf{n}}\right)$, we consider the expectation value $\langle\hat{n}\rangle_{\tilde{\varrho}_{\mathrm{p},\mathbf{n}}} := \mathrm{Tr}\left[\hat{n}\,\tilde{\varrho}_{\mathrm{p},\mathbf{n}}\right]$. We write $\mathbb{1}$ for the identity operator. From the facts $\mathbb{1} - |\mathbf{0}\rangle\langle\mathbf{0}| \leq \hat{n}$ and $\tilde{\varrho}_{\mathrm{p},\mathbf{n}} \geq 0$, it follows that

$$\begin{aligned} \langle\hat{n}\rangle_{\tilde{\varrho}_{\mathrm{p},\mathbf{n}}} &= \mathrm{Tr}\left[\sum_{\mathbf{n}} n|\mathbf{n}\rangle\langle\mathbf{n}|\tilde{\varrho}_{\mathrm{p},\mathbf{n}}\right] \\ &\geq \mathrm{Tr}\left[(\mathbb{1} - |\mathbf{0}\rangle\langle\mathbf{0}|)\tilde{\varrho}_{\mathrm{p},\mathbf{n}}\right] \\ &= \mathrm{Tr}\left[\tilde{\varrho}_{\mathrm{p},\mathbf{n}}\right] - F \end{aligned} \tag{18}$$

and hence,

$$F \geq F^{(\mathbf{n})} := \langle\mathbb{1} - \hat{n}\rangle_{\tilde{\varrho}_{\mathrm{p},\mathbf{n}}}. \tag{19}$$

For $\varrho_{\mathrm{p}} = \varrho_{\mathrm{t}}$ it holds that $\langle\hat{n}\rangle_{\tilde{\varrho}_{\mathrm{p},\mathbf{n}}} = 0$ and $\mathrm{Tr}\left[\tilde{\varrho}_{\mathrm{p},\mathbf{n}}\right] = 1$. Thus, for $\varrho_{\mathrm{p}} = \varrho_{\mathrm{t}}$ the inequality in equation (18) becomes an equality and, therefore, the bound in equation (19) is then saturated, as announced earlier.

Next, we define the operator valued Pochhammer-symbol

$$p_t(\hat{n}_j) := \hat{n}_j(\hat{n}_j - 1)(\hat{n}_j - 2)\cdots(\hat{n}_j - t), \tag{20}$$

for any integer $t \geq 0$, and $p_{-1}(x) := 1$. In Supplementary Note 6 we show that

$$\left(\hat{a}_j^{\dagger}\right)^{n_j} \hat{n}_j (\hat{a}_j)^{n_j} = p_{n_j}(\hat{n}_j), \tag{21a}$$

and

$$\left(\hat{a}_j^{\dagger}\right)^{n_j} (\hat{a}_j)^{n_j} = p_{n_j-1}(\hat{n}_j). \tag{21b}$$

Inserting equation (17) into equation (19), using the cyclicity property of the trace, grouping the operators of each mode together, using equation (21a) and equation (21b), and that $p_t(\hat{n}_j) = p_{t-1}(\hat{n}_j)(\hat{n}_j - t)$, we obtain the general fidelity lower bound

$$F \geq F^{(\mathbf{n})} = \frac{1}{\mathbf{n}!} \left\langle (n + 1 - \hat{n}) \prod_{j=1}^{m} p_{n_j-1}(\hat{n}_j) \right\rangle_{\tilde{\varrho}_{\mathrm{p}}}, \tag{22}$$

where $\mathbf{n}! := n_1! n_2! \ldots n_m!$.

In order to specialize to the linear-optical case $\varrho_{\mathrm{t}} \in \mathcal{C}_{\mathrm{LO}}$, we take $\mathbf{n} = \mathbf{1}_n$, i.e., $n_j = 1$ for all $j \in [n]$ and $n_j = 0$ otherwise. With this, $F^{(\mathbf{n})}$ in equation (22) simplifies to the bound $F^{(n)}$ in equation (6). Finally, to restrict it to the Gaussian case $\varrho_{\mathrm{t}} \in \mathcal{C}_{\mathrm{G}}$, we take $n_j = 0$ for all $j \in [m]$. This yields the particularly simple expression

$$F \geq F^{(0)} := 1 - \langle\hat{n}\rangle_{\tilde{\varrho}_{\mathrm{p}}}. \tag{23}$$

The last expression manifests the above-mentioned connection between our fidelity lower bound and an intuitive extremality property of Gaussian states. Namely, the lower the average number of photons of $\tilde{\varrho}_{\mathrm{p}}$ is, the closer to the vacuum it must be and, therefore, the closer ϱ_{p} to the target state ϱ_{t}.

Arthur does not have, in general, enough quantum capabilities to directly estimate $\langle\hat{n}\rangle_{\tilde{\varrho}_{\mathrm{p}}}$ by undoing the operation $\hat{U}$ on Merlin's outputs and then measuring $\hat{n}$ in the Fock-state basis. However, we show in the next section that he can efficiently obtain $\langle\hat{n}\rangle_{\tilde{\varrho}_{\mathrm{p}}}$, as well as the expectation values in equations (22) and (6), from the results of single-mode homodyne or heterodyne measurements.

Measurement scheme. First, we introduce some notation. By $\hat{q}_j$ and $\hat{p}_j$ we denote, respectively, the conjugated position and momentum phase-space quadrature operators of the jth mode in the canonical convention[42,43], that is, with the commutation relations $\left[\hat{q}_j, \hat{p}_{j'}\right] = \mathrm{i}\,\delta_{j,j'}$. The particle number operator of the jth mode can be written in terms of the phase-space quadratures as $\hat{n}_j = \hat{q}_j^2 + \hat{p}_j^2 - 1/2$. In addition, it will be convenient to group all quadrature operators into a $2m$-component column vector $\hat{\mathbf{r}}$, with elements

$$\hat{r}_{2j-1} := \hat{q}_j \quad \text{and} \quad \hat{r}_{2j} := \hat{p}_j. \tag{24}$$

As already mentioned, the action of $\hat{U}$ on mode space is given by a symplectic matrix $\mathbf{S} \in \mathrm{Sp}(2m, \mathbb{R})$ and a displacement vector $\mathbf{x} \in \mathbb{R}^{2m}$. More precisely, under a Gaussian unitary $\hat{U}$, $\hat{\mathbf{r}}$ transforms according to the affine linear map[42]

$$\hat{\mathbf{r}} \mapsto \hat{U}^{\dagger}\hat{\mathbf{r}}\hat{U} = \mathbf{S}\hat{\mathbf{r}} + \mathbf{x}. \tag{25}$$

Equivalently, the right-hand side of this equation defines the Heisenberg representation of $\hat{\mathbf{r}}$ with respect to $\hat{U}$. In addition, it will be useful to denote the Heisenberg representation of $\hat{\mathbf{r}}$ with respect to $\hat{U}^{\dagger}$ by $\hat{\tilde{\mathbf{r}}} := \hat{U}\hat{\mathbf{r}}\hat{U}^{\dagger}$. Thanks to equation (25), we can write $\hat{\tilde{\mathbf{r}}}$ in terms of the symplectic matrix $\mathbf{S}$ and displacement vector $\mathbf{x}$ that define $\hat{U}$, as

$$\hat{\tilde{\mathbf{r}}} = \mathbf{S}^{-1}(\hat{\mathbf{r}} - \mathbf{x}). \tag{26}$$

The symbols $\hat{r}^2 := \hat{\mathbf{r}}^T\hat{\mathbf{r}}$ and $\hat{\tilde{r}}^2 := \hat{\tilde{\mathbf{r}}}^T\hat{\tilde{\mathbf{r}}}$ will represent, respectively, the scalar products of $\hat{\mathbf{r}}$ and $\hat{\tilde{\mathbf{r}}}$ with themselves. Also, we will use the same notation for the

Heisenberg representations of each quadrature operator with respect to $\hat{U}^\dagger$, that is, $\hat{\tilde{q}}_j := \hat{U}^\dagger \hat{q}_j \hat{U}$ and $\hat{\tilde{p}}_j := \hat{U}^\dagger \hat{p}_j \hat{U}$.

Next, for $\beta \in \{0, n, \mathbf{n}\}$, we express our fidelity bounds in the general form

$$F^{(\beta)} = \left\langle \hat{F}^{(\beta)} \right\rangle_{\varrho_{\mathrm{p}}}, \tag{27}$$

where $\hat{F}^{(\beta)}$ is an observable decomposed explicitly in terms of the local observables to which Arthur has access. We start with the Gaussian case $\varrho_{\mathrm{t}} \in \mathcal{C}_{\mathrm{G}}$. To express the bound of equation (23) as in equation (27), we first write the total photon-number operator as

$$\hat{n} = \sum_{j=1}^{m} \hat{n}_j = \sum_{j=1}^{m} \left(\hat{q}_j^2 + \hat{p}_j^2 - \frac{1}{2} \right) = \hat{r}^2 - \frac{m}{2}. \tag{28}$$

This, in combination with equation (23), yields

$$\hat{F}^{(0)} = 1 - \left(\hat{\tilde{r}}^2 - \frac{m}{2} \right). \tag{29}$$

Note that, due to equation (26), each component of $\hat{\mathbf{r}}$ is a linear combination of at most $2m$ components of $\hat{\mathbf{r}}$. This implies that Arthur can obtain $\left\langle \hat{\tilde{r}}^2 \right\rangle_{\varrho_{\mathrm{p}}}$ by measuring at most $2m$ single-quadrature expectation values of the form $\langle \hat{r}_k \rangle_{\varrho_{\mathrm{p}}}$ and $4m^2$ second moments of the form $\Gamma^{(1)}_{k,k'} := \left\langle \frac{1}{2}(\hat{r}_k \hat{r}_{k'} + \hat{r}_{k'} \hat{r}_k) \right\rangle_{\varrho_{\mathrm{p}}}$. He can then classically efficiently combine them as dictated by $\mathbf{S}$ and $\mathbf{x}$ in equation (26). In Supplementary Note 1, we give the details of this measurement procedure, which we call $\mathcal{M}_{\mathrm{G}}$, and show that measuring $m\kappa$ second moments, instead of $4m^2$, is actually enough. Furthermore, in Supplementary Note 4, we show that only $m+3$ experimental settings suffice if homodyne detection is used and a single setting if heterodyne detection is used.

Now, proceeding in a similar manner with the generic bound of equation (22), we obtain

$$\hat{F}^{(\mathbf{n})} = \frac{1}{\mathbf{n}!} \left[n + 1 - \left(\hat{\tilde{r}}^2 - \frac{m}{2} \right) \right] \prod_{j=1}^{m} p_{n_j - 1} \left(\hat{\tilde{q}}_j^2 + \hat{\tilde{p}}_j^2 - \frac{1}{2} \right). \tag{30}$$

Note that the observable in equation (29) is contained as the special case $n = 0$. For target states in the class $\mathcal{C}_{\mathrm{LO}}$, $\hat{U}$ is assumed to be a passive Gaussian unitary. Such unitaries preserve the area in phase-space, that is, if $\varrho_{\mathrm{t}} \in \mathcal{C}_{\mathrm{LO}}$ it holds that $\hat{\tilde{r}}^2 = \hat{r}^2$ (for details, see Supplementary Note 1). Hence, using this and specialising to the case $\mathbf{n} = \mathbf{1}_n$, equation (30) simplifies to

$$\hat{F}^{(n)} = \left[n + 1 - \left(\hat{r}^2 - \frac{m}{2} \right) \right] \prod_{j=1}^{n} \left(\hat{\tilde{q}}_j^2 + \hat{\tilde{p}}_j^2 - \frac{1}{2} \right). \tag{31}$$

Again by virtue of equation (26), Arthur can now obtain the expectation values of the observables in equations (30) and (31) by measuring $2j$th moments of the form $\Gamma^{(j)}_{k_1,l_1,\ldots,k_j,l_j} := \left\langle \frac{1}{2^j} (\hat{r}_{k_1} \hat{r}_{l_1} + \hat{r}_{l_1} \hat{r}_{k_1}) \cdots (\hat{r}_{k_j} \hat{r}_{l_j} + \hat{r}_{l_j} \hat{r}_{k_j}) \right\rangle_{\varrho_{\mathrm{p}}}$ and then classically recombining them, which—for constant n—he can do efficiently. In Supplementary Note 1, we give the details of the measurement procedure to obtain $F^{(n)}$, which we call $\mathcal{M}_{\mathrm{LO}}$. In particular, we show that, to obtain $\left\langle \hat{F}^{(n)} \right\rangle_{\varrho_{\mathrm{p}}}$, estimating a total of $\mathrm{O}(m(4d^2+1)^n)$ $2j$th moments, with $j \in [n+1]$, is enough. Also, we list which moments are the relevant ones in terms of $\varrho_{\mathrm{t}} \in \mathcal{C}_{\mathrm{LO}}$. Furthermore, in Supplementary Note 4, we show that a single heterodyne experimental setting throughout suffices here too.

Finally, in Supplementary Note 2, we derive a bound analogous to that of equations (27) and (31) for post-selected target states $\varrho_{\mathcal{S}_{\mathrm{t}}}$. More precisely, we show that the fidelity $F_{\mathcal{S}} := F\left(\varrho_{\mathcal{S}_{\mathrm{t}}}, \varrho_{\mathcal{S}_{\mathrm{p}}}\right)$ between $\varrho_{\mathcal{S}_{\mathrm{t}}}$ and an arbitrary, unknown $(m-a)$-mode system preparation $\varrho_{\mathcal{S}_{\mathrm{p}}}$ is lower bounded as

$$F_{\mathcal{S}} \geq F^{(n)}_{\mathcal{S}} = \left\langle \hat{F}^{(n)}_{\mathcal{S}} \right\rangle_{\varrho_{\mathcal{S}_{\mathrm{p}}}}, \tag{32}$$

$$\hat{F}^{(n)}_{\mathcal{S}} := \frac{\langle \mathbf{n}_{\mathcal{A}}|_{\mathcal{A}} \hat{F}^{(n)} |\mathbf{n}_{\mathcal{A}}\rangle_{\mathcal{A}}}{\mathbb{P}(\mathbf{n}_{\mathcal{A}}|\varrho_{\mathrm{t}})}. \tag{33}$$

Actually, the bound holds not only for target states $\varrho_{\mathrm{t}} \in \mathcal{C}_{\mathrm{LO}}$ projected onto $|\mathbf{n}_{\mathcal{A}}\rangle_{\mathcal{A}}$ but also for the more general target states of equation (14), with $\hat{U}$ any Gaussian unitary and $|\mathbf{n}\rangle$ any Fock-basis state, projected onto any generic a-mode pure product state on $\mathcal{A}$. Apart from being experimentally more relevant, linear-optical network target states post-selected with Fock-basis measurements possess the peculiarity that the corresponding bound is tight for perfect preparations. That is, for these states, if $\varrho_{\mathcal{S}_{\mathrm{p}}} = \varrho_{\mathcal{S}_{\mathrm{t}}}$ then $F^{(n)}_{\mathcal{S}} = F_{\mathcal{S}} = 1$, just as in the cases without post-selection.

Non-Gaussian state nullifiers. It is instructive to mention that the observables

$$\hat{N}^{(0)}_j := \hat{\tilde{q}}_j^2 + \hat{\tilde{p}}_j^2 - 1/2, \tag{34}$$

for $j \in [m]$, correspond to the so-called nullifiers of the Gaussian states in $\mathcal{C}_{\mathrm{G}}$. The nullifiers are commuting operators that, despite originally introduced[51] as a tool to define Gaussian graph states, can be tailored to define any pure Gaussian state[52,53]: If a state is the simultaneous null-eigenvalue eigenstate of all m nullifiers of a given pure Gaussian state, then the former is necessarily equal to the latter. The bound $F^{(0)}$, given by equations (27) and (29), exploits the fact that if a preparation gives a sufficiently low expectation value for the sum $\sum_{j=1}^{m} \hat{N}^{(0)}_j$ of all m nullifiers, then its fidelity with the target state must be high. A similar intuition has been previously exploited[12,13] to experimentally check for multimode entanglement of ultralarge Gaussian cluster states. Here we cannot only certify entanglement but the quantum state itself.

Analogously, in the non-Gaussian case, from the derivation of equation (30) and the fact that

$$\frac{1}{\mathbf{n}!} \mathrm{Tr} \left[\prod_{j=1}^{m} p_{n_j - 1} \left(\hat{\tilde{q}}_j^2 + \hat{\tilde{p}}_j^2 - 1/2 \right) \varrho_{\mathrm{p}} \right] = \mathrm{Tr} \left[\tilde{\varrho}_{\mathrm{p},\mathbf{n}} \right] \tag{35}$$

equals 1 for $\varrho_{\mathrm{p}} = \varrho_{\mathrm{t}}$, we can identify the observable

$$\hat{N}^{(\mathbf{n})}_j := \frac{1}{\mathbf{n}!} \left(\hat{\tilde{q}}_j^2 + \hat{\tilde{p}}_j^2 - \frac{1}{2} - n_j \right) \prod_{k=1}^{m} p_{n_k - 1} \left(\hat{\tilde{q}}_k^2 + \hat{\tilde{p}}_k^2 - 1/2 \right) \tag{36}$$

as the jth nullifier of the m-mode non-Gaussian state ϱ_{t} of equation (14). Indeed, all m observables given by equation (36) for all $j \in [m]$ commute and have ϱ_{t} as their unique, simultaneous null-eigenvalue eigenstate. To end up with, due to the projection onto $|\mathbf{n}_{\mathcal{A}}\rangle_{\mathcal{A}}$, the equivalent observables for $\varrho_{\mathcal{S}_{\mathrm{t}}} \in \mathcal{C}_{\mathrm{PLO}}$ do not in general commute. Nevertheless, their linear combination given by $1 - \hat{F}^{(n)}_{\mathcal{S}}$ still defines an observable with $\varrho_{\mathcal{S}_{\mathrm{t}}}$ as its unique null-eigenvalue eigenstate. These observables constitute, to our knowledge[42,52,53], the first examples of nullifiers for non-Gaussian states.

References

1. Giovannetti, V., Lloyd, S. & Maccone, L. Advances in quantum metrology. *Nat. Photon.* **5,** 222–229 (2011).
2. Nielsen, M. & Chuang, I. *Quantum Computation and Quantum Information* (Cambridge Univ. Press, 2000).
3. Schindler, P. *et al.* Experimental repetitive quantum error correction. *Science* **332,** 1059–1061 (2011).
4. Barends, R. *et al.* Superconducting quantum circuits at the surface code threshold for fault tolerance. *Nature* **508,** 500–503 (2014).
5. Cirac, J. I. & Zoller, P. Goals and opportunities in quantum simulation. *Nat. Phys.* **8,** 264–266 (2012).
6. Aspuru-Guzik, A. & Walther, P. Photonic quantum simulators. *Nat. Phys.* **8,** 285–291 (2012).
7. Bloch, I., Dalibard, J. & Nascimbéne, S. Quantum simulations with ultra-cold quantum gases. *Nat. Phys.* **8,** 267–276 (2012).
8. Blatt, R. & Roos, C. F. Quantum simulations with trapped ions. *Nat. Phys.* **8,** 277–284 (2012).
9. Houk, A. A., Türeci, H. E. & Koch, J. On-chip quantum simulation with superconducting circuits. *Nat. Phys.* **8,** 292–299 (2012).
10. Yao, X.-C. *et al.* Observation of eight-photon entanglement. *Nat. Photon.* **6,** 225–228 (2012).
11. Huang, Y.-F. *et al.* Experimental generation of an eight-photon Greenberger-Horne-Zeilinger state. *Nat. Commun.* **2,** 546 (2012).
12. Chen, M., Menicucci, N. C. & Pfister, O. Experimental realisation of multipartite entanglement of 60 modes of the quantum optical frequency comb. *Phys. Rev. Lett.* **112,** 120505–120509 (2014).
13. Yokoyama, S. *et al.* Optical generation of ultra-large-scale continuous-variable cluster states. *Nat. Photon.* **7,** 982–986 (2013).
14. Spring, J. B. *et al.* Boson sampling on a photonic chip. *Science* **339,** 798–801 (2013).
15. Tillmann, M. *et al.* Experimental boson sampling. *Nat. Photon.* **7,** 540–544 (2013).
16. Broome, M. A. *et al.* Photonic boson sampling in a tunable circuit. *Science* **339,** 794–798 (2013).
17. Crespi, A. *et al.* Integrated multimode interferometers with arbitrary designs for photonic boson sampling. *Nat. Photon.* **7,** 545–549 (2013).
18. Peruzzo, A. *et al.* Quantum walks of correlated photons. *Science* **329,** 1500–1503 (2010).
19. Crespi, A. *et al.* Anderson localization of entangled photons in an integrated quantum walk. *Nat. Photon.* **7,** 322–328 (2013).
20. Gogolin, C., Kliesch, M., Aolita, L. & Eisert, J. Boson sampling in the light of sample complexity. Preprint at http://arxiv.org/abs/1306.3995(2013).
21. Aaronson, S. & Arkhipov, A. BosonSampling is far from uniform. Preprint at http://arxiv.org/abs/1309.7460(2013).
22. Spagnolo, N. *et al.* Experimental validation of photonic boson sampling. *Nat. Photon.* **8,** 615–620 (2014).
23. Carolan, J. *et al.* On the experimental verification of quantum complexity in linear optics. *Nat. Photon.* **8,** 621 (2014).
24. Tichy, M. C., Mayer, K., Buchleitner, A. & Molmer, K. Stringent and efficient assessment of Boson-Sampling devices. *Phys. Rev. Lett.* **113,** 020502–020506 (2014).

25. Gross, D., Liu, Y.-K., Flammia, S. T., Becker, S. & Eisert, J. Quantum state tomography via compressed sensing. *Phys. Rev. Lett.* **105,** 150401–150404 (2010).
26. Aharonov, D., Ben-Or, M. & Eban, E. Interactive proofs for quantum computation. Preprint at http://arxiv.org/abs/0810.5375(2008).
27. Broadbent, A., Fitzsimons, J. & Kashefi, E. Universal blind quantum computation. *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2009)* 517 (Atlanta, GA, 2009).
28. Fitzsimons, J. & Kashefi, E. Unconditionally verifiable blind computation. Preprint at http://arxiv.org/abs/1203.5217 (2012).
29. Kapourniotis, T., Kashefi, E. & Datta., A. Verified delegated quantum computing with one pure qubit. Preprint at http://arxiv.org/abs/1403.1438(2014).
30. Toth, G. *et al.* Permutationally invariant quantum tomography. *Phys. Rev. Lett.* **105,** 250403–250406 (2010).
31. Cramer, M. *et al.* Efficient quantum state tomography. *Nat. Commun.* **1,** 149 (2010).
32. Flammia, S. T. & Liu, Y.-K. Direct fidelity estimation from few Pauli measurements. *Phys. Rev. Lett.* **106,** 230501–230504 (2011).
33. da Silva, M. P., Landon-Cardinal, O. & Poulin, D. Practical characterisation of quantum devices without tomography. *Phys. Rev. Lett.* **107,** 210404–210407 (2011).
34. Flammia, S. T., Gross, D., Liu, Y.-K. & Eisert, J. Quantum tomography via compressed sensing: Error bounds, sample complexity, and efficient estimators. *N. J. Phys.* **14,** 095022–095051 (2012).
35. Magesan, E., Gambetta, J. M. & Emerson, J. Scalable and robust randomized benchmarking of quantum processes. *Phys. Rev. Lett.* **106,** 180504–180507 (2011).
36. Dell'Anno, F., De Siena, S., Albano, L. & Illuminati, F. Continuous-variable quantum teleportation with non-Gaussian resources. *Phys. Rev. A* **76,** 022301–022311 (2007).
37. Navarrete-Benlloch, C., García-Patrón, R., Shapiro, J. H. & Cerf, N. J. Enhancing quantum entanglement by photon addition and subtraction. *Phys. Rev. A* **86,** 012328–012336 (2012).
38. Dell'Anno, F. *et al.* Tunable non-Gaussian resources for continuous-variable quantum technologies. *Phys. Rev. A* **88,** 043818–043830 (2013).
39. Eisert, J., Browne, D. E., Scheel, S. & Plenio, M. B. Distillation of continuous-variable entanglement. *Ann. Phys. (NY)* **311,** 431–458 (2004).
40. Knill, E., Laflamme, R. & Milburn, G. J. A scheme for efficient quantum computation with linear optics. *Nature* **409,** 46–52 (2001).
41. Kok, P. *et al.* Linear optical quantum computing with photonic qubits. *Rev. Mod. Phys.* **79,** 135–174 (2007).
42. Weedbrook, C. *et al.* Gaussian quantum information. *Rev. Mod. Phys.* **84,** 621–669 (2012).
43. Eisert, J. & Plenio, M. B. Introduction to the basics of entanglement theory in continuous-variable systems. *Int. J. Quant. Inf* **1,** 479–506 (2003).
44. Pirandola, S., Eisert, J., Weedbrook, C., Furusawa, A. & Braunstein, S. L. Advances in quantum teleportation. *Nat. Photon.* **9,** 641–652 (2015).
45. Braunstein, S. L. Squeezing as an irreducible resource. *Phys. Rev. A* **71,** 055801–055804 (2005).
46. Reck, M., Zeilinger, A., Bernstein, H. J. & Bertani, P. Experimental realization of any discrete unitary operator. *Phys. Rev. Lett.* **73,** 58–61 (1994).
47. Mari, A. & Eisert, J. Positive Wigner functions render classical simulation of quantum computation efficient. *Phys. Rev. Lett.* **109,** 230503–230507 (2012).
48. Veitch, V., Ferrie, C., Gross, D. & Emerson, J. Negative quasi-probability as a resource for quantum computation. *N. J. Phys.* **14,** 113011 (2012).
49. Veitch, V., Wiebe, N., Ferrie, C. & Emerson, J. Efficient simulation scheme for a class of quantum optics experiments with non-negative Wigner representation. *N. J. Phys.* **15,** 013037 (2013).
50. Aaronson, S. & Arkhipov, A. The computational complexity of linear optics. *Theory Comput.* **9,** 143 (2013).
51. Gu, M., Weedbrook, C., Menicucci, N. C., Ralph, T. C. & van Loock, P. Quantum computing with continuous-variable clusters. *Phys. Rev. A* **79,** 062318–062333 (2009).
52. Aolita, L., Roncaglia, A., Ferraro, A. & Acín, A. Gapped two-body Hamiltonian for continuous-variable quantum computation. *Phys. Rev. Lett.* **106,** 090501–090504 (2010).
53. Menicucci, N. C., Flammia, S. T. & van Loock, P. Graphical calculus for Gaussian pure states. *Phys. Rev. A* **83,** 042335–042357 (2011).

Acknowledgements

We thank F.G.S.L. Brandão and S.T. Flammia for discussions on certification of state preparation, and M. Cramer for noticing an error in a previous version of the manuscript. We thank the EU (RAQUEL, SIQS, AQuS, REQS—Marie Curie IEF No 299141), the BMBF, the FQXI, the Studienstiftung des Deutschen Volkes, MPQ-ICFO, the Spanish project FOQUS, the Generalitat de Catalunya (SGR 875), and FOQUS for support.

Author contributions

All authors participated in all the discussions and contributed with insights. L.A. conceived the fidelity bound and its estimation technique. L.A., C.G. and M.K. carried out all the calculations and worked out the details of the formalism.

Additional information

Supplementary Information accompanies this paper at http://www.nature.com/naturecommunications

Competing financial interests: The authors declare no competing financial interests.

Reprints and permission information is available online at http://npg.nature.com/reprintsandpermissions/

How to cite this article: Aolita, L. *et al.* Reliable quantum certification of photonic state preparations. *Nat. Commun.* 6:8498 doi: 10.1038/ncomms9498 (2015).