Efficient Verification of Continuous-Variable Quantum States and Devices without Assuming Identical and Independent Operations

Ya-Dong Wu,[1] Ge Bai,[1] Giulio Chiribella,[1,2,3,4] and Nana Liu[5,6,7,*]

[1]QICI Quantum Information and Computation Initiative, Department of Computer Science, The University of Hong Kong, Pokfulam Road, Hong Kong

[2]The University of Hong Kong Shenzhen Institute of Research and Innovation, 5/F, Key Laboratory Platform Building, No. 6, Yuexing 2nd Road, Nanshan, Shenzhen 518057, China

[3]Department of Computer Science, Parks Road, Oxford OX1 3QD, United Kingdom

[4]Perimeter Institute for Theoretical Physics, Waterloo, Ontario N2L 2Y5, Canada

[5]Institute of Natural Sciences, Shanghai Jiao Tong University, Shanghai 200240, China

[6]Ministry of Education, Key Laboratory in Scientific and Engineering Computing, Shanghai Jiao Tong University, Shanghai 200240, China

[7]University of Michigan-Shanghai Jiao Tong University Joint Institute, Shanghai 200240, China

(Received 20 December 2020; accepted 18 May 2021; published 16 June 2021)

Continuous-variable quantum information, encoded into infinite-dimensional quantum systems, is a promising platform for the realization of many quantum information protocols, including quantum computation, quantum metrology, quantum cryptography, and quantum communication. To successfully demonstrate these protocols, an essential step is the certification of multimode continuous-variable quantum states and quantum devices. This problem is well studied under the assumption that multiple uses of the same device result in identical and independently distributed (i.i.d.) operations. However, in realistic scenarios, identical and independent state preparation and calls to the quantum devices cannot be generally guaranteed. Important instances include adversarial scenarios and instances of time-dependent and correlated noise. In this Letter, we propose the first set of reliable protocols for verifying multimode continuous-variable entangled states and devices in these non-i.i.d scenarios. Although not fully universal, these protocols are applicable to Gaussian quantum states, non-Gaussian hypergraph states, as well as amplification, attenuation, and purification of noisy coherent states.

DOI: 10.1103/PhysRevLett.126.240503

Introduction.—Continuous-variable (CV) quantum information protocols are widely used in quantum optics [1,2]. To realize these protocols, it is essential to be able to perform state and device verification on CV states and devices [3]. State verification [4–12] addresses the problem of whether or not a state generated by a quantum device is close enough to a specified target state. While some efficient protocols exist [4,7], they require the tested systems to be identically and independently (i.i.d) prepared, an assumption that is hard to guarantee in realistic scenarios. Quantum device verification [13] is the problem of determining whether the outputs of a quantum device are close to associated target output states, averaged over all possible input states. CV quantum device verification in the non-i.i.d setting has so far been an open problem. In this Letter, we propose verification protocols for multimode CV entangled states and CV quantum devices in non-i.i.d scenarios.

For finite dimensional systems, quantum state and quantum device characterization schemes in the non i.i.d setting have received increasing attention in recent years, motivated by applications in quantum computing and quantum networks with noisy intermediate-scale quantum devices [14–17]. There are two important classes of scenarios where the i.i.d assumption cannot be made. The first class includes adversarial scenarios, in which we cannot trust that the adversary will necessarily allow us access to multiple copies of the same state, or to multiple uses of the same quantum device. This situation can occur, for instance, in verifiable blind quantum computing [18], where malicious servers can send entangled states to the client to steer computational results. A second class of scenarios involves the presence of time-dependent noise, which can exhibit correlations between subsequent uses of the same device. This situation occur, for example, in the transmission of photons through an optical fiber, whose birefringence fluctuates over time [19]. In all these cases, we cannot trust that a realistic quantum device will output identical and independently prepared states in each run.

In the non-i.i.d setting for qubits, a powerful method is to employ the quantum de Finetti theorem, which enables one to approximate a collection of non-i.i.d states by a smaller number of copies of i.i.d states after a randomizing procedure followed by tracing out a subsystem [20]. Leveraging

this result, one can reduce the problem of non-i.i.d verification to the i.i.d scenario. A similar strategy can be used for CV state verification. In the CV setting, there are two main classes of quantum de Finetti theorems, which can be separated into finite dimensional approximations [21], and infinite dimensional constructions [22]. The existing finite dimensional approximations have been developed for applications in quantum key distribution, typically involving single mode systems, and have an exponential scaling of the error in the dimension parameter. On the other hand, in the infinite dimensional constructions one lacks a simple, practically implementable randomizing procedure required by the de Finetti theorem to enable the non-i.i.d state to be approximated by i.i.d states. To circumvent these issues, we develop a finite dimensional approximation that can be used for multimode states and has a polynomial scaling of the error with the dimension parameter.

In our approach, we propose a new method, which can be used to verify a broad class of CV quantum states, including multimode Gaussian states and CV hypergraph states. Unlike previous approaches, which used permutation symmetry by randomly reshuffling the various systems, our test takes advantage of an additional symmetry property, namely, symmetry with respect to rotations in phase space [23]. This additional symmetry allows us to overcome all the challenges of the non-i.i.d. setting. In our protocol, the initial non-i.i.d state is randomized not only by a random permutation, but also by random phase rotations at each subsystem. These rotations can be performed without loss of generality owing to the symmetry of the states under consideration. Exploiting this rotational symmetry, we are able to achieve polynomial scaling of the approximation error between the randomized non-i.i.d state and its i.i.d approximation with respect to an effective finite dimension d associated to the family of states under consideration.

Building on our i.i.d approximation, we then construct a verification protocol with the desirable properties of soundness and completeness, which are necessary for successful verification. Soundness of a protocol means that the probability of false positives is low: if the actual state is orthogonal to the target state, it should have a low probability of passing the verification test. Completeness means that the correct state has a high probability to pass the test. Thanks to rotational symmetry, we show that the complexity of our verification protocol has a favourable scaling in terms of the soundness and completeness parameters.

Building on our CV verification results, we also provide the first protocol for CV non-i.i.d quantum device verification. This protocol combines a duality between state tests and channel tests introduced in Ref. [24] and our new techniques in CV state verification. With these ingredients, we can demonstrate bounds on the completeness and soundness of device verification.

Framework.—We now introduce the necessary basics of CV quantum states and the task of verification, before going on to demonstrate explicitly our protocols for specific classes of CV states and channels.

A CV state lies on an infinite dimensional Hilbert space, equipped with observables with a continuous spectrum, such as the position and momentum observables of a quantum particle. CV states are usually implemented by bosonic systems, described by quantum harmonic oscillators. CV quantum information is encoded in the tensor product $\mathcal{H}^{\otimes k}$ of Hilbert space $\mathcal{H} = \mathrm{Span}\{|n\rangle\}_{n\in\mathbb{N}}$, where $\hat{n}|n\rangle = n|n\rangle$ is a particle number eigenstate with particle number operator $\hat{n} = \hat{a}^\dagger\hat{a}$. Quadrature operators are $\hat{q} := [(\hat{a} + \hat{a}^\dagger)/\sqrt{2}]$ and $\hat{p} := [(\hat{a} - \hat{a}^\dagger)/\sqrt{2}\mathrm{i}]$. For k-mode CV states, the quadrature operators are denoted by vector $\hat{\boldsymbol{x}} := (\hat{q}_1, \hat{p}_1, \ldots, \hat{q}_k, \hat{p}_k)$.

An important class of CV states are Gaussian states. Pure Gaussian states can be written in the form $U_{\boldsymbol{S},\boldsymbol{d}}|0\rangle^{\otimes k}$, where $U_{\boldsymbol{S},\boldsymbol{d}}$ is a Gaussian unitary operation, characterized by an affine mapping $(\boldsymbol{S},\boldsymbol{d}):\hat{\boldsymbol{x}} \to \boldsymbol{S}\hat{\boldsymbol{x}} + \boldsymbol{d}$, where $\boldsymbol{S} \in \mathbb{R}^{2k\times 2k}$ is a symplectic transformation and $\boldsymbol{d} \in \mathbb{R}^{2k}$.

The most common CV measurement is homodyne detection [25], which is routinely implemented in quantum optics laboratories. Mathematically, the homodyne measurement corresponds to a projective measurement of a quadrature operator. This means that the expectation value of any linear combination of quadratures $\hat{q}(\theta) := \cos\theta\hat{q} + \sin\theta\hat{p}$ and $\hat{p}(\theta) := -\sin\theta\hat{q} + \cos\theta\hat{p}$, with $\theta \in [0, \pi/2)$, can be measured using homodyne detection in a rotated basis.

In state verification, a verifier has to test the preparation of a target state, denoted by $|\phi\rangle \in \mathcal{H}^{\otimes k}$, where $k \in \mathbb{N}^+$. The verifier is given n quantum registers, whose state is claimed to consist of n identical copies of the target state. The actual state of the n registers is unknown to the verifier, and is denoted by $\rho^{(n)} \in \mathcal{S}(\mathcal{H}^{\otimes k\cdot n})$. The state $\rho^{(n)}$ could deviate from the ideal state $|\phi\rangle\langle\phi|^{\otimes n}$ due to imperfections of the source, or could even be prepared by a potentially malicious server. The verifier then chooses $n - m$ quantum registers uniformly at random, and performs measurements on each register, to decide whether the reduced state at the remaining m registers is close enough to $|\phi\rangle\langle\phi|^{\otimes m}$ or not. From now on, we use the term randomly choosing to mean choosing from an uniform random distribution. Denoting $0 \le T \le \mathbb{1}$ as the POVM element on $\mathcal{H}^{\otimes k(n-m)}$ that corresponds to the verification test flagged as passed, and $0 < \epsilon_s, \epsilon_c < \frac{1}{2}$ as failure probabilities, a reliable quantum state verification scheme must satisfy (i) soundness: for any permutation-invariant $\rho \in \mathcal{S}(\mathcal{H}^{\otimes k\cdot n})$, $\mathrm{tr}(T \otimes (\mathbb{1} - |\phi\rangle\langle\phi|^{\otimes m})\rho) \le \epsilon_s$, and (ii) completeness: $\mathrm{tr}(T|\phi\rangle\langle\phi|^{\otimes(n-m)}) \ge 1 - \epsilon_c$. Intuitively, a good bound on soundness denotes a low probability of a false positive, that is, a low joint probability that the test is passed and yet the remaining state is orthogonal to the target state. On the

other hand, completeness guarantees that if the state is identical to the target state, it must pass the verification test with a high probability.

The task of quantum device verification, closely related to state verification, is to determine whether the outputs of a quantum device are close to target output states or not, when averaged over a fiducial ensemble of input states. We can define an ensemble of input states as $\{p_x, \rho_x\}_{x\in X}$, where X is an index set, $\{p_x\}_{x\in X}$ is a probability distribution, and $\rho_x \in \mathcal{S}(\mathcal{H}^{\otimes k})$. Suppose the target outputs are pure states $\{|\phi\rangle_x\}_{x\in X}$, where $|\phi\rangle_x \in \mathcal{H}^{\otimes k}$. A target channel $\mathcal{E}_t$ is defined as the quantum channel that achieves the maximal average fidelity $\bar{F}(\mathcal{E}) \coloneqq \sum_{x\in X} p_x \langle\phi_x|\mathcal{E}(\rho_x)|\phi_x\rangle$, and its maximum achievable value is denoted by $\bar{F}_{\max}$ [26,27].

In this context, an important observation is that any test of quantum devices can be realized by preparing a single entangled state on the input and an ancillary system, and to perform a single joint measurement on the output and the ancillary system [24]. This observation yields a general device verification protocol similar to state verification above. Let $\mathcal{E}^{(n)}$ be an $n \cdot k$-mode quantum channel, claimed to act as n independent uses of the k-mode target channel $\mathcal{E}_t$. Here we regard $\mathcal{E}^{(n)}$ as a channel with n inputs, each input consisting of k modes. The verifier then randomly chooses $(n-m)$ inputs and injects one part of a bipartite entangled state into each of these inputs. Then, the verifier can apply local measurements at the outputs and the ancillary systems, to determine whether the channel $\mathcal{E}^{(m)}$ at the remaining m inputs is close to $\mathcal{E}_t^{\otimes m}$ or not.

A reliable device verification scheme must similarly satisfy soundness and completeness conditions (i) soundness: for any permutation-invariant n-input channel $\mathcal{E}^{(n)}$,

$$\left[T \otimes \left(\mathbb{1} - \frac{\bar{F}^{\otimes m}}{\bar{F}_{\max}^{m}}\right)\right](\mathcal{E}^{(n)}) \leq \epsilon_s, \tag{1}$$

where T is the map from an $(n-m)$-input quantum channel to the probability of passing the test, and 1 is a map that maps any m-input channel into the number 1. (ii) completeness:

$$T(\mathcal{E}_t^{\otimes(n-m)}) \geq 1 - \epsilon_c. \tag{2}$$

The soundness of channel verification is analogous to that of state verification, except here the figure of merit is average fidelity instead of fidelity between the prepared state and the target state.

State verification under the i.i.d assumption can be performed by detecting a fidelity witness W, which is an observable whose expectation value with respect to any prepared state is a tight lower bound of its fidelity with the target state. This provides an efficient approach to verify both CV quantum states [4,7] and CV quantum channels [13]. In this Letter, although we do not have the i.i.d assumption, we will continue to use these techniques after obtaining an i.i.d approximation.

To obtain an i.i.d approximation using a finite d de Finetti theorem, one needs to filter CV states so they effectively lie on a d-dimensional subspace. We note that although one cannot infer whether all the remaining subsystems are bounded to lie on a finite d-dimensional subspace by testing partial subsystems, it is possible to deduce whether a CV state is bounded for most subsystems. Then through randomization in terms of both permutation and phase rotations, this almost-bounded CV state is then close to an i.i.d d-dimensional state, after tracing out part of its subsystems.

In general non-i.i.d settings, CV quantum state verification comprises of two subprotocols: the dimension test and the fidelity test. The dimension test is used to bound the dimension d. In the dimension test, the measurement outcomes of homodyne detection are compared with a certain threshold. If the measurement outcomes are always less than the threshold, this gives a strong guarantee that each subsystem is confined in a subspace spanned by Fock states $|n\rangle$ with n less than d. Through discarding a large fraction of the subsystems of the randomized non-i.i.d state, one can treat the state at the remaining subsystems as approximately i.i.d, due to a finite-d de Finetti theorem. After getting an i.i.d approximation, the fidelity test, similar to the test under i.i.d assumption, is to certify the fidelity between the state at each remaining subsystem and the target state, by detecting the fidelity witness at partial subsystems. Figure 1 summarizes the key steps of the scheme.

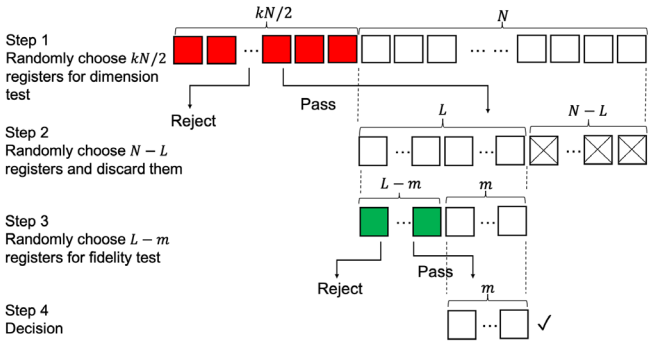

FIG. 1. The verifier receives $(k/2+1)N$ registers, each of which is represented by a box and contains an unknown k-mode state. The verifier randomly chooses $kN/2$ registers, represented by red boxes, to apply a dimension test. If the dimension test is passed, then the verifier goes on with the fidelity test at the other N registers. Otherwise, the verifier aborts the test (rejects). Suppose the dimension test is passed. Then, the verifier randomly chooses $N-L$ registers, represented by boxes with crosses inside, and discards them. For the remaining registers, the verifier randomly chooses $L-m$ registers, represented by green boxes, to perform the fidelity test. If the fidelity test is passed, then the verifier takes the state in the remaining m registers, represented by blank boxes, as reliable copies of target state $|\psi\rangle$. Otherwise, the verifier rejects the remaining states.

The verification protocol.—Suppose the target state $|\phi\rangle = U|0\rangle^{\otimes k}$ is a multimode entangled state, mathematically obtained by applying a suitable unitary operator U to the vacuum. Given $(k/2+1)N$ quantum registers, each of which stores a k-mode quantum state, the verifier uses $kN/2$ registers for the dimension test. Here N is chosen to be an even integer. The first step of the dimension test is to divide the $kN/2$ registers into k groups of $N/2$ registers each. In each group, by comparing the square of homodyne detection outcomes with an upper bound $d_0/2 > 0$ for $N/2$ registers, the verifier infers whether most of the k-mode states in the remaining N registers fall on a finite-dimensional subspace $\bar{\mathcal{H}}_j := \{U|n_i\rangle^{\otimes k}_{i=1} |\ \forall\ i, n_i \in \mathbb{N}, n_j < d_0\}$ of $\mathcal{H}^{\otimes k}$, where $1 \le j \le k$. If the k groups all pass the test, then most subsystems at the remaining N registers fall on a finite-dimensional subspace $\bar{\mathcal{H}} := \cap_{j=1}^{k} \bar{\mathcal{H}}_j$ of $\mathcal{H}^{\otimes k}$. Then after discarding a large fraction of the remaining N registers and keeping only L registers ($L \ll N$), the reduced state $\rho^{(L)}$ at the remaining L registers can be shown to fall on $\bar{\mathcal{H}}^{\otimes L}$ and is approximately i.i.d to high probability. Proofs of these statements can be found in the Supplemental Material [28]. Finally, the verifier chooses $L-m$ of the remaining registers to perform the fidelity test. Here one estimates the expectation value of chosen fidelity witness $\mathbb{1} - U\hat{n}U^\dagger$ at $L-m$ registers. The outcome of the fidelity then determines whether the fidelity between the states at the remaining m registers and the tensor product of m target states is close to one. We will later explain the detailed procedure of the dimension test and the fidelity test for specific target states.

At each round of testing, each register is randomly chosen and this randomization guarantees permutation invariance of the registers. Besides permutational symmetry, our verification test also exhibits an additional symmetry, owing to the fact that the vacuum state $|0\rangle^{\otimes k} = U^\dagger|\phi\rangle$ is invariant under rotations in phase space. This additional symmetry is enforced by first applying the unitary operation $U^\dagger$, and then applying a homodyne detection in a randomly rotated quadrature basis at each mode. Practically, for certain unitaries U like Gaussian unitary operations, the application of the unitary gate $U^\dagger$ can be omitted, because it can be reproduced by classical processing of the measurement outcomes. Because of this rotational symmetry, only the diagonal entries of any $\rho^{(kN/2+N)} \in \mathcal{L}(\mathcal{H}^{\otimes k(kN/2+N)})$ in the basis $\{U|n_i\rangle^{\otimes k}_{i=1}\}^{\otimes(kN/2+N)}$ affects the results of this test.

Now we describe the dimension test in detail for pure Gaussian target states. In the dimension test, the verifier divides $kN/2$ registers into k groups. In jth group ($j \in [k]$), the verifier randomly chooses phase $\theta_l \in [0, (\pi/2))$ ($l \in [N/2]$) at each register and measures either $\hat{\tilde{q}}_j(\theta_l)$ or $\hat{\tilde{p}}_j(\theta_l)$, where $\hat{\tilde{q}}_j = \sum_{1\le i\le 2k} \boldsymbol{S}^\top_{2j-1,i}(\hat{\boldsymbol{x}}_i - \boldsymbol{d}_i)$, and $\hat{\tilde{p}}_j = \sum_{1\le i\le 2k} \boldsymbol{S}^\top_{2j,i}(\hat{\boldsymbol{x}}_i - \boldsymbol{d}_i)$ are both linear combinations of local quadrature operators. Repeat the measurement in each group for $N/2$ times, and denote the lth measurement outcome in the jth group by $f_{j,l}$. For each measurement outcome, the verifier defines an associated variable $z_{j,l}$: if $(f_{j,l})^2 > d_0/2$, $z_{j,l} = 1$; otherwise, $z_{j,l} = 0$. After homodyne measurements on the $kN/2$ registers, if for all $j \in [k]$, $\sum_{l=1}^{N/2} z_{j,l} \le N\mathrm{e}^{-c_0^2 d_0}$, with $c_0 = 1 - (1/\sqrt{2})$, then the states are considered to have passed the dimension test; otherwise, the verifier aborts the test as soon as any j fails the $\sum_{l=1}^{N/2} z_{j,l} \le N\mathrm{e}^{-c_0^2 d_0}$ condition and rejects all the states.

If the states pass the dimension test, then the verifier randomly chooses $L = \lceil 264k^2m^2d_0^2\ln(4/\epsilon)/\epsilon^2 + m\rceil$ from the remaining registers, where $0 < \epsilon < 1/2$ is a tolerant failure probability, and discards all the other registers. These registers are now used for the fidelity test, where the verifier first randomly chooses $L-m$ registers from the L registers. At the ith register ($i \in [L-m]$), the verifier then randomly chooses $j_i \in [k]$ and $\theta_i \in [0, (\pi/2))$, and measures either $\hat{\tilde{q}}_{j_i}(\theta_i)$ or $\hat{\tilde{p}}_{j_i}(\theta_i)$ randomly. Denote the measurement outcome by χ_i. After $L-m$ rounds of measurements, the verifier compares an estimator of the fidelity witness $W^* = 1 + k/2 - k/(L-m)\sum_{i=1}^{L-m}\chi_i^2$ with threshold $1-(\epsilon/2m)$. If $W^* \ge 1-(\epsilon/2m)$, the verifier accepts the state at remaining m registers as reliable copies of $|\phi\rangle$. Otherwise, the verifier rejects.

This scheme also works for verification of non-Gaussian CV hypergraph states [10,42], where the verifier follows the same procedure, except that $\hat{\tilde{q}}_j := U\hat{q}_jU^\dagger$ and $\hat{\tilde{p}}_j := U\hat{p}_jU^\dagger$ are different from above.

Theorem.—Suppose $|\phi\rangle = U|0\rangle^{\otimes k}$ is a k-mode entangled state, where U satisfies that U followed by homodyne detections can be simulated by homodyne detections followed by classical processing of measurement outcomes. When

$$10k\mathrm{e}^{-c_0^2 d_0}\left(\frac{264k^2m^2d_0^2\ln\frac{4}{\epsilon}}{\epsilon^2} + m\right) \le \epsilon \tag{3}$$

and

$$N > \frac{50}{64}\ln\frac{4k}{\epsilon}\mathrm{e}^{2c_0^2 d_0}, \tag{4}$$

this verification scheme, characterized by T, satisfies soundness, i.e., for any permutation-invariant $\rho \in \mathcal{S}(\mathcal{H}^{\otimes k\cdot n})$, $\mathrm{tr}(T \otimes (\mathbb{1} - |\phi\rangle\langle\phi|^{\otimes m})\rho) \le \epsilon$, and completeness, i.e., $\mathrm{tr}(T|\phi\rangle\langle\phi|^{\otimes((k/2+1)N-m)}) \ge 1-\epsilon$.

The sample complexity of this verification scheme is

$$(k/2+1)N = O\left[\frac{k^7m^4}{\epsilon^6}\mathrm{Poly}\left(\ln\frac{km}{\epsilon}\right)\right], \tag{5}$$

which can be considered as a theoretical upper bound of the minimum required samples for the most general scenarios

without energy cutoffs. Compared to the sample complexity $L = O\{(k^2m^2/\epsilon^2)\mathrm{Poly}[\ln(km/\epsilon)]\}$ in the i.i.d case, at most L^4 samples are sufficient for CV-state verification in non-i.i.d scenario. In experiments, unknown quantum states can be sent to the verifier through light pulses, and the verifier implements the verification test by applying homodyne detections on the sequence of pulses. If we assume that each mode is confined in a subspace spanned by Fock states $|n\rangle$ with $n < d_0$, then the sample complexity is reduced to $O[(k^4m^2d_0^4 \ln 1/\epsilon)/\epsilon^3]$. Using state-of-the-art homodyne detections [43,44], for $k^4d_0^4 \lesssim [10^{13}\epsilon^3/(m^2 \ln 1/\epsilon)]$, the verification test can be accomplished within a few hours.

These same state verification techniques can also be used to implement the verification of quantum devices. We begin with the observation that any test of quantum devices can be realized by preparing one entangled state on the input and an ancillary system, and then jointly measuring the output and the ancillary system [24]. The observable to be measured can then be chosen to be (average) fidelity witness as in a state verification task [13]. By adding a dimension test and rotational symmetry in the fidelity test, we get our quantum-device verification schemes. Verification protocols of amplification, attenuation, and purification of noisy coherent states can be found in the Supplemental Material [28].

Corollary.—Suppose the target device $\mathcal{E}_t$ is an optimal quantum device for amplification, attenuation, or purification of noisy coherent states, or a unitary U satisfying that U followed by homodyne detections can be simulated by homodyne detections followed by classical processing of measurement outcomes, and the ensemble state of input is a Gaussian state. Then when d_0 and N satisfy Eqs. (3) and (4), respectively, the verification scheme satisfies soundness (1) and completeness (2) with $n = (k/2 + 1)N$ and $\epsilon_s = \epsilon_c = \epsilon$.

A verification scheme of k-mode quantum devices has the same sample complexity as shown in Eq. (5).

Conclusions.—We have proposed the first protocols that can verify both multimode CV entangled states and CV quantum devices without the assumption of i.i.d state and device preparation and bounded statistical moments of quadratures. Through bypassing the i.i.d assumption for multimode states, our results can be applied to CV blind quantum computing [7,45,46], where a potentially malicious server may deceive an agent or steer the computational results by preparing entangled states. Our results can also be applied to performance benchmarks of quantum devices [24,26,27,47–52], in a broader setting where the devices may undergo arbitrary correlated noise processes in subsequent uses, and may contain an internal memory that affects their behavior on later inputs.

The authors are grateful to Barry C. Sanders (University of Calgary), Carlos Navarrete-Benlloch (Shanghai Jiao Tong University), and Huangjun Zhu (Fudan University) for interesting and fruitful discussions. Y. D. W., G. B., and G. C. acknowledge funding from the National Natural Science Foundation of China Grant No. 11675136, and the Hong Kong Research Grant Council Grants No. 17300918 and No. 17307520. N. L. acknowledges funding from the Shanghai Pujiang Talent Grant (No. 20PJ1408400) and the NSFC International Young Scientists Project (No. 12050410230). N. L. is also supported by the Innovation Program of the Shanghai Municipal Education Commission (No. 2021-01-07-00-02-E00087), the Shanghai Municipal Science and Technology Major Project (2021SHZDZX0102) and the Natural Science Foundation of Shanghai Grant No. 21ZR1431000.

*Corresponding author.
nana.liu@quantumlah.org

[1] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).
[2] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
[3] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, and E. Kashefi, Nat. Rev. Phys. **2**, 382 (2020).
[4] L. Aolita, C. Gogolin, M. Kliesch, and J. Eisert, Nat. Commun. **6**, 8498 (2015).
[5] S. Pallister, N. Linden, and A. Montanaro, Phys. Rev. Lett. **120**, 170502 (2018).
[6] Y. Takeuchi and T. Morimae, Phys. Rev. X **8**, 021060 (2018).
[7] N. Liu, T. F. Demarie, S.-H. Tan, L. Aolita, and J. F. Fitzsimons, Phys. Rev. A **100**, 062309 (2019).
[8] H. Zhu and M. Hayashi, Phys. Rev. Lett. **123**, 260504 (2019).
[9] H. Zhu and M. Hayashi, Phys. Rev. Applied **12**, 054047 (2019).
[10] Y. Takeuchi, A. Mantri, T. Morimae, A. Mizutani, and J. F. Fitzsimons, npj Quantum Inf. **5**, 27 (2019).
[11] U. Chabaud, T. Douce, F. Grosshans, E. Kashefi, and D. Markham, in *15th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2020)*, Leibniz International Proceedings in Informatics (LIPIcs), Vol. 158, edited by S. T. Flammia (Schloss Dagstuhl–Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 2020), pp. 3:1–3:15.
[12] U. Chabaud, F. Grosshans, E. Kashefi, and D. Markham, arXiv:2006.03520.
[13] Y.-D. Wu and B. C. Sanders, New J. Phys. **21**, 073026 (2019).
[14] M. Christandl and R. Renner, Phys. Rev. Lett. **109**, 120403 (2012).
[15] C. Pfister, M. A. Rol, A. Mantri, M. Tomamichel, and S. Wehner, Nat. Commun. **9**, 27 (2018).
[16] J. J. Wallman, Quantum **2**, 47 (2018).

[17] A. Erhard, J. J. Wallman, L. Postler, M. Meth, R. Stricker, E. A. Martinez, P. Schindler, T. Monz, J. Emerson, and R. Blatt, Nat. Commun. **10**, 5347 (2019).
[18] A. Gheorghiu, T. Kapourniotis, and E. Kashefi, Theory Comput. Syst. **63**, 715 (2019).
[19] J. L. Ball and K. Banaszek, J. Phys. A **39**, L1 (2006).
[20] M. Christandl, R. König, G. Mitchison, and R. Renner, Commun. Math. Phys. **273**, 473 (2007).
[21] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).
[22] A. Leverrier, J. Math. Phys. (N.Y.) **59**, 042202 (2018).
[23] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, Phys. Rev. Lett. **110**, 030502 (2013).
[24] G. Bai and G. Chiribella, Phys. Rev. Lett. **120**, 150502 (2018).
[25] H.-A. Bachor and T. C. Ralph, *A Guide to Experiments in Quantum Optics* (Wiley Online Library, New Jersey, 2004).
[26] G. Chiribella and J. Xie, Phys. Rev. Lett. **110**, 213602 (2013).
[27] Y. Yang, G. Chiribella, and G. Adesso, Phys. Rev. A **90**, 042319 (2014).
[28] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.126.240503 for proof of main results and examples of verification schemes, which includes Refs. [29–41].
[29] M. Rossi, M. Huber, D. Bruß, and C. Macchiavello, New J. Phys. **15**, 113022 (2013).
[30] T. Morimae, Y. Takeuchi, and M. Hayashi, Phys. Rev. A **96**, 062321 (2017).
[31] R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A **68**, 022312 (2003).
[32] M. Gu, C. Weedbrook, N. C. Menicucci, T. C. Ralph, and P. van Loock, Phys. Rev. A **79**, 062318 (2009).
[33] M. J. Bremner, A. Montanaro, and D. J. Shepherd, Phys. Rev. Lett. **117**, 080501 (2016).
[34] T. Douce, D. Markham, E. Kashefi, E. Diamanti, T. Coudreau, P. Milman, P. van Loock, and G. Ferrini, Phys. Rev. Lett. **118**, 070503 (2017).
[35] J. M. Arrazola, P. Rebentrost, and C. Weedbrook, arXiv:1712.07288.
[36] R. C. Pooser, A. M. Marino, V. Boyer, K. M. Jones, and P. D. Lett, Phys. Rev. Lett. **103**, 010501 (2009).
[37] U. L. Andersen, R. Filip, J. Fiurášek, V. Josse, and G. Leuchs, Phys. Rev. A **72**, 060301(R) (2005).
[38] P. Marek and R. Filip, Quantum Inf. Comput. **7**, 609 (2007).
[39] X. Zhao and G. Chiribella, Phys. Rev. A **95**, 042303 (2017).
[40] M. Tomamichel and A. Leverrier, Quantum **1**, 14 (2017).
[41] R. J. Serfling, Ann. Stat. **2**, 39 (1974).
[42] D. W. Moore, Phys. Rev. A **100**, 062301 (2019).
[43] Y. Shaked, Y. Michael, R. Z. Vered, L. Bello, M. Rosen-bluh, and A. Pe'er, Nat. Commun. **9**, 609 (2018).
[44] S. Takeda and A. Furusawa, APL Photonics **4**, 060902 (2019).
[45] T. Morimae, Phys. Rev. Lett. **109**, 230502 (2012).
[46] K. Marshall, C. S. Jacobsen, C. Schäfermeier, T. Gehring, C. Weedbrook, and U. L. Andersen, Nat. Commun. **7**, 13795 (2016).
[47] R. Namiki, M. Koashi, and N. Imoto, Phys. Rev. Lett. **101**, 100502 (2008).
[48] S. L. Braunstein, C. A. Fuchs, and H. J. Kimble, J. Mod. Opt. **47**, 267 (2000).
[49] K. Hammerer, M. M. Wolf, E. S. Polzik, and J. I. Cirac, Phys. Rev. Lett. **94**, 150503 (2005).
[50] M. Owari, M. B. Plenio, E. S. Polzik, A. Serafini, and M. M. Wolf, New J. Phys. **10**, 113014 (2008).
[51] G. Adesso and G. Chiribella, Phys. Rev. Lett. **100**, 170503 (2008).
[52] G. Chiribella and G. Adesso, Phys. Rev. Lett. **112**, 010501 (2014).