Client-friendly continuous-variable blind and verifiable quantum computing

Nana Liu,[1,2,3,*] Tommaso F. Demarie,[4,2,3,†] Si-Hui Tan,[2,3] Leandro Aolita,[5,6] and Joseph F. Fitzsimons[2,3]

[1]*John Hopcroft Center for Computer Science, Shanghai Jiao Tong University, Shanghai 200240, China*
[2]*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543*
[3]*Singapore University of Technology and Design, 8 Somapah Road, Singapore 487372*
[4]*Entropica Labs, 32 Carpenter Street, Singapore 059911*
[5]*Instituto de Física, Universidade Federal do Rio de Janeiro, Caixa Postal 68528, 21941-972 Rio de Janeiro, RJ, Brazil*
[6]*ICTP South American Institute for Fundamental Research, Instituto de Física Teórica,*
UNESP-Universidade Estadual Paulista R. Dr. Bento T. Ferraz 271, Bl. II, São Paulo 01140-070, SP, Brazil

(Received 7 July 2018; published 5 December 2019)

We present a verifiable and blind protocol for assisted universal quantum computing on continuous-variable (CV) platforms. This protocol is experimentally friendly to the client, as it only requires Gaussian-operation capabilities from the latter. Moreover, the server does not require universal quantum-computational power either, its only function being to supply the client with copies of a single-mode non-Gaussian state. Universality is attained based on state injection of the server's non-Gaussian supplies. The protocol is automatically blind because the non-Gaussian resource requested to the server is always the same, regardless of the specific computation. Verification, in turn, is possible thanks to an efficient non-Gaussian state fidelity test where we assume identical state preparation by the server. It is based on Gaussian measurements by the client on the injected states, which is potentially interesting on its own. The division of quantum hardware between client and server assumed here is in agreement with the experimental constraints expected in realistic schemes for CV cloud quantum computing.

DOI: 10.1103/PhysRevA.100.062309

I. INTRODUCTION

Quantum computers promise computational speedups for crucial classically intractable problems. This includes the simulation of complex many-body quantum systems [1–3], searching through unstructured databases [4], machine learning and artificial intelligence [5–8], and cryptography [9,10]. Similarly to the early classical computers, full quantum-computing capabilities are initially expected only at a few remote locations. Cloud quantum computing will then offer a means for clients to delegate their computations to a distant server with more powerful quantum hardware.

Delegating a computation, however, raises important security and privacy issues, which motivated *verifiable and blind assisted quantum computing*. Ideally, the client, Alice, would like to delegate a computation to an untrusted server, Bob, while maintaining the privacy of her computation. At the same time, Alice needs a reliable certificate of the correctness of the computational output. The former property is known as *blindness* and the latter as *verifiability* [11]. After the first proposals [12–14], which required repeated rounds of interaction between Alice and Bob, several improvements and variations followed [13,15–27]. Importantly, preliminary experimental studies of assisted quantum computing have also been conducted [28–31].

All of these developments have taken place in the qubit regime. In contrast, blind quantum computing on continuous-variable (CV) hardware is a much less explored territory [32,33]. To the best of our knowledge there is a single proposal reported [32] that allows the client to hide her input, output, and her computation [1]. CV degrees of freedom offer a competitive alternative to encode quantum information [34–36], with some remarkable advantages over qubit-based platforms with highly desirable features for assisted computations [2]. CV schemes have also been explored in a variety of settings [37–43]. Unfortunately, the seminal protocol of [32] puts a huge burden on Alice's shoulders in terms of experimental requirements and, in addition, requires repeated interaction between Alice and Bob.

More precisely, the protocol of [32] requires that Alice performs single-mode *non-Gaussian* operations, while delegating the Gaussian entangling gates to Bob. However, single-mode non-Gaussian operations are among the most experimentally challenging ones [44–47]. On the contrary, *Gaussian* operations—including maximally entangling gates—are the most experimentally accessible ones for CV systems [36,48]. They play a role analogous to Clifford operations in qubit systems. Like Clifford group operations on stabilizer states, any Gaussian CV computation can be efficiently simulated classically [49], while any single non-Gaussian operation is enough to boost Gaussian quantum computations to universal ones [50]. Up to now, no CV scheme for blind quantum

[*] nana.liu@quantumlah.org
[†] tommaso@entropicalabs.com

[1] We note that the scheme in [33] shows only the encryption of the input.

[2] For instance, CVs offer higher detection efficiencies and can be integrated into existing optical-fiber networks [36].

computing has been reported which is experimentally friendly to the client.

In this article we fill this gap. We derive a verifiable and blind scheme for universal quantum computation on CV systems that requires only Gaussian quantum hardware on Alice's side. In addition, it requires neither repeated interaction between Alice and Bob nor universal quantum hardware on Bob's side. Bob only needs to prepare one kind of single-mode non-Gaussian state, e.g., the celebrated cubic phase state created by applying cubic phase gates [44–47] onto the vacuum. We assume an honest Bob is restricted to preparing identical copies of the cubic phase state. The difference in quantum hardware between Alice and Bob considered here reflects more fairly the actual constraints of real-life experiments. With this, our protocol lays the theoretical groundwork for realistic CV quantum cloud computing schemes.

II. BACKGROUND

For a multimode CV state, let $\hat{x}_k$ and $\hat{p}_\ell$ be the position and momentum operators of the k^{th} and ℓ^{th} modes, respectively. These then satisfy the commutation relations $[\hat{x}_k, \hat{p}_\ell] = i\delta_{k,\ell}$. A quantum operation is said to be Gaussian when it is generated by a unitary $U = \exp(-iH)$, where the Hamiltonian H is a second-order polynomial in the mode operators. An example is single-mode squeezing $S(s) = e^{i\ln(s)(\hat{x}\hat{p}+\hat{p}\hat{x})}$ for $s \in \mathbb{R}$. Gaussian states are created by applying Gaussian operations onto the vacuum state. Gaussian measurements are an important subset of Gaussian operations and yield Gaussian distributed outcomes when applied to Gaussian states. These include homodyne detection which consists of the measurement of the quadrature $\hat{x}$ or $\hat{p}$ of a mode.

To implement an arbitrary U, acting on an m-mode state $|\Psi_{\text{in}}\rangle$, one requires only the set of Gaussian operations $\mathcal{G}$, including Gaussian measurements $\mathcal{M}$, and just one type of non-Gaussian operation [50]. Thus, U can be divided into sequences of Gaussian operations and non-Gaussian gates of the form $\mathbb{1}_k \otimes C(\gamma) \otimes \mathbb{1}_{m-k-1}$, where $0 \leqslant k \leqslant m-1$. Here $\mathbb{1}_k \equiv \mathbb{1}^{\otimes k}$ where $\mathbb{1}$ is the single-mode identity operator.

An example of a non-Gaussian operation that is needed for universality is the single-mode cubic phase gate $C(\gamma) = e^{i\gamma\hat{x}^3}$, where $\gamma \in \mathbb{R}$. When $|0\rangle$ is the single-mode vacuum state, this gives rise to the following non-Gaussian state:

$$|\tilde{\gamma}\rangle_s = C(\tilde{\gamma})S(s)|0\rangle = \frac{e^{i\tilde{\gamma}\hat{x}^3}e^{-\hat{x}^2/(2s^2)}}{\sqrt{s}\pi^{1/4}}\int dx|x\rangle. \qquad (1)$$

This is a finitely squeezed variant of the originally proposed cubic phase state [51]. We will later employ these as Bob's resource states for our assisted computation protocol.

We now discuss three important notions for an assisted computation protocol: *correctness*, *blindness*, and *verifiability*. In contrast to the discrete-variable case, here even if Bob is honest and there is no noise, the outcome is intrinsically probabilistic due to the fact that the resource state is finitely squeezed. Hence, we must adapt the following definitions of correctness and verifiability to account for this.

Definition 1 (δ correctness). Let $|\Psi_{\text{out}}(\mathbf{y})\rangle$ denote the m-mode state that is the outcome of the intended computation that Alice wants to perform, where $\mathbf{y}$ denotes the string of measurement results of the computation device that the outcome could depend on. Then $\Pi_{\text{correct}} = |\Psi_{\text{out}}(\mathbf{y})\rangle\langle\Psi_{\text{out}}(\mathbf{y})|$ is the projector onto the correct outcome of Alice's computation. Let $\sigma_{\text{out}}(\mathbf{y})$ be the outcome of Alice's computation when she delegates part of her computation to Bob *and* Bob is honest. Then we say our delegation protocol is δ correct for $0 \leqslant \delta \leqslant 1$ [3] when the average probability of $\sigma_{\text{out}}(\mathbf{y})$ being projected onto the correct outcomes satisfies

$$\int d\mathbf{y}\text{Tr}[\Pi_{\text{correct}}\sigma_{\text{out}}(\mathbf{y})]P(\sigma_{\text{out}}(\mathbf{y})) \geqslant \delta, \qquad (2)$$

where $P(\sigma_{\text{out}}(\mathbf{y}))$ is the probability of obtaining measurement result $\mathbf{y}$ if Bob is honest. So if Bob is honest, Alice obtains the correct outcome to her computation with high probability if δ is large.

Definition 2 (blindness). A delegation protocol is said to be *blind* if the input state, the operations performed, and the output state remain hidden from Bob (see [11] and references therein for a formal definition).

Definition 3 (ϵ verifiability). Let $\rho_{\text{out}}(\mathbf{y})$ be the resulting outcome of this computation. The probability of $\rho_{\text{out}}(\mathbf{y})$ projecting onto incorrect outcomes of the computation is denoted $P(\text{incorrect}) = \text{Tr}(\Pi_{\text{incorrect}}\rho_{\text{out}}(\mathbf{y}))$, where $\Pi_{\text{incorrect}} = \mathbb{1}_m - |\Psi_{\text{out}}(\mathbf{y})\rangle\langle\Psi_{\text{out}}(\mathbf{y})|$. Let $P(\text{accept})$ be the probability that Alice *accepts* the resource state given by Bob, according to her verification test. Then the assisted computation is said to be ϵ verifiable (for $0 \leqslant \epsilon \leqslant 1$) if the average joint probability $\int d\mathbf{y}P(\text{incorrect} \cap \text{accept})P(\mathbf{y}) \leqslant \epsilon$, where $P(\mathbf{y})$ is the probability of obtaining measurement result $\mathbf{y}$ for the accepted resource state.

III. BLIND DELEGATION AND VERIFICATION PROTOCOL

Alice wishes to perform an arbitrary CV quantum computation with output $U|\Psi_{\text{in}}\rangle$, where U is a generic CV unitary operation and $|\Psi_{\text{in}}\rangle$ the m-mode Gaussian input state. Alice only requests the same cubic phase state from Bob. Thus, blindness is an intrinsic, built-in feature of the scheme and only an upper bound on the number of cubic phase gates in the computation is revealed to Bob. Verification, in turn, is based on a novel non-Gaussian state fidelity witness specially tailored for the cubic phase state, inspired by the witnesses of [52]. This is measured by Alice on a subset of Bob's supplied states, used as test set. Remarkably, the witness requires only Gaussian measurements on at most four homodyne-detection bases per test mode, which is interesting in its own right. In addition, to estimate the expectation value of the witness, we use importance sampling techniques [53], which allow the test-set size required for verifiability to scale only quadratically with the number of cubic phase states consumed by the computation. Hence, our protocol is not only experimentally friendly to Alice but also efficient in the number of single-mode non-Gaussian resource states required. We summarize our blind delegation and verification protocol below.

Protocol 1. Verified and blind assisted CV quantum computation.

Alice's resources are as follows.

[3] Similar to definition in [68].

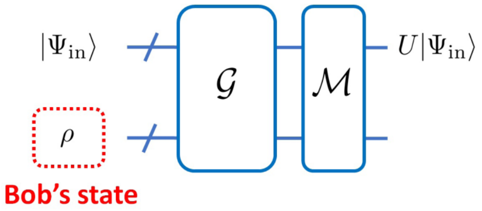

FIG. 1. Universal CV quantum computation. To implement an arbitrary CV computation $U|\Psi_{\rm in}\rangle$, one requires only Gaussian operations and at least one non-Gaussian operation. The non-Gaussian operation can be implemented by Alice when she uses Bob's non-Gaussian state resource ρ and applies unitary Gaussian operations $\mathcal{G}$ and Gaussian measurements $\mathcal{M}$. See Fig. 2 and the text for more details.

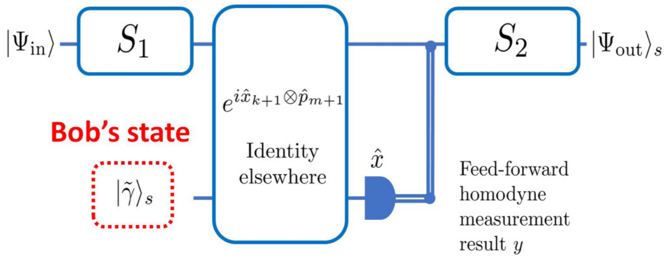
$|\Psi_{\rm in}\rangle$
S_1
$e^{i\hat{x}_{k+1}\otimes\hat{p}_{m+1}}$
Identity elsewhere
S_2
$|\Psi_{\rm out}\rangle_s$
Bob's state
$|\tilde{\gamma}\rangle_s$
$\hat{x}$
Feed-forward homodyne measurement result y

FIG. 2. Alice's circuit to implement a cubic phase gate. Alice implements an approximation to the cubic phase gate $\mathbb{1}_k \otimes C(\gamma) \otimes \mathbb{1}_{m-k-1}$ acting on the state $|\Psi_{\rm in}\rangle$ by using the resource state $|\tilde{\gamma}\rangle_s$ given by Bob. Here $C(\gamma)$ acts on the $(k+1)^{\rm th}$ mode of $|\Psi_{\rm in}\rangle$ and the resource state is on the $(m+1)^{\rm th}$ mode. Here $S(r)$ is the single-mode squeezing operator with $r = (\gamma/\tilde{\gamma})^{1/3}$, where the value r is only known to Alice. The initial gate $S_1 \equiv \mathbb{1}_k \otimes S(r) \otimes \mathbb{1}_{m-k-1}$ and final gate $S_2 \equiv \mathbb{1}_k \otimes S^{\dagger}(r)G^{-1}(y) \otimes \mathbb{1}_{m-k-1}$ acting on the top register are used to hide the value of γ from Bob. Here $G^{-1}(y) = e^{-i\tilde{\gamma}y^3}e^{-3i\tilde{\gamma}y\hat{x}(\hat{x}+y)}$ is a Gaussian operator and y is the measurement outcome on the lower register of the operator $\hat{x}$.

(a) A m-mode Gaussian state, $|\Psi_{\rm in}\rangle$ which is the input state for her computation.

(b) A circuit description representing Gaussian measurements and a unitary operation U that is decomposed into Gaussian gates and M cubic phase gates.

(c) Parameters chosen for the verification test: threshold fidelity $F_T < 1$ (minimum fidelity permitted for the fidelity between states σ and ρ defined below), significance level β (i.e., maximum failure probability of the test), and an estimation error η (with respect to the quantity $F_{\rm low}$ defined below) that satisfies $\eta \leqslant (1 - F_T)/2$.

(1) Alice requests $(N+1)$ copies of the pure state $\sigma = (|\tilde{\gamma}\rangle_s\langle\tilde{\gamma}|_s)^{\otimes M}$ from Bob. We will see later how N scales with M, β, and η.

(2) Bob sends to Alice $(N+1)$ copies of an M-mode state ρ. If he is honest, $\rho = \sigma$. If Bob is dishonest, he sends Alice the state $\rho^{\otimes(N+1)}$ where $\rho \neq \sigma$ and we assume he cannot send more general states.

(3) Alice retains the state ρ for her computation and runs the verification test on the remaining N copies of ρ. For the verification test, Alice makes an estimate $F_{\rm low}^{(\rm est)}$ of the quantity $F_{\rm low} \equiv \mathrm{Tr}(\mathcal{W}\rho)$. The observable $\mathcal{W}$ is a fidelity witness for the state σ, given in Eq. (5). The quantity $F_{\rm low}$ is a lower bound on the fidelity $F(\sigma, \rho)$ between ρ and σ. It can be estimated up to precision η with homodyne detection on $\rho^{\otimes N}$, following the details of the importance sampling method in Appendix D. We say Alice *rejects* $\rho^{\otimes N}$ if $F_{\rm low}^{(\rm est)} < F_T + \eta$ and *accepts* otherwise.

(4) If Alice *accepts*, she uses the remaining state ρ for her computation. More precisely, she uses ρ to perform M cubic phase gates on her input state $|\Psi_{\rm in}\rangle$ by means of a gate teleportation protocol [4]. See Figs. 1 and 2.

When Bob is honest, gate teleportation and Gaussian operations allow Alice to approximately implement $C(\gamma)$ on any desired mode of her input state $|\Psi_{\rm in}\rangle$. This protocol is both δ correct and blind as shown by the following theorem.

Theorem 1. Our assisted computation protocol is δ correct with $\delta = 1$ and reveals to Bob only an upper bound on the number of cubic phase states used.

Proof. Our assisted computation protocol relies on the gate teleportation protocol in Fig. 2. If the m-mode input state in the top register is $|\Psi_{\rm in}\rangle$, then the m-mode output state in the top register is $|\Psi_{\rm out}\rangle_s = (\mathbb{1}_k \otimes g_{s/r}(y/r)C(\gamma) \otimes \mathbb{1}_{m-k-1})|\Psi_{\rm in}\rangle$, where $g_s(y) = e^{-(\hat{x}+y)^2/(2s^2)}$ and y is the measurement result in the bottom register. The gate teleportation protocol thus enables the application of a non-Gaussian operation on $|\Psi_{\rm in}\rangle$. More specifically, it applies a cubic phase gate on the $(k+1)^{\rm th}$ mode of $|\Psi_{\rm in}\rangle$ up to a Gaussian factor for $k = 0, 1, \ldots, m-1$ [51,54]. For this protocol we can write $\Pi_{\rm correct} = |\Psi_{\rm out}\rangle_s\langle\Psi_{\rm out}|_s$. Thus $\mathrm{Tr}(\Pi_{\rm correct}|\Psi_{\rm out}\rangle_s\langle\Psi_{\rm out}|_s) = 1$. Then $\int d\mathbf{y}\mathrm{Tr}(\Pi_{\rm correct}\sigma_{\rm out}(\mathbf{y}))P(\sigma_{\rm out}(\mathbf{y})) = 1$ and we have perfect correctness, i.e., $\delta = 1$ in Eq. (2). See Appendix A for more details.

We note that if Bob's resource state is the infinitely squeezed version of the cubic phase state, the output state of Fig. 2 becomes exactly the cubic phase gate applied to the initial state $|\Psi_{\rm in}\rangle$, since $s \rightarrow \infty$ implies $g_s(y) \rightarrow 1$. Although finite s gives a correction term to the cubic phase gate, this does not change our correctness argument since we only desire to perform a fixed non-Gaussian gate and not necessarily exactly the cubic phase gate.

To show blindness in the sense that Bob can only learn the upper bound on the number of cubic states used, we first note that Bob has no access to any Gaussian part of the computation, which includes the input state $|\Psi_{\rm in}\rangle$ and the results of the (Gaussian) measurements. Furthermore, he cannot reconstruct the exact value of the parameters γ used by Alice during the computation since Alice decides the squeezing parameter $r = (\gamma/\tilde{\gamma})^{1/3}$ used. This means the only useful information Bob obtains is the number of resource states that Alice requests, which is an upper bound on the size of the computation. ■

Now we describe Alice's verification test, which is based on the notion of fidelity witnesses [52,53,55,56]. These witnesses bypass the need for full state tomography [57] of Bob's state. They allow for verification in the general setting of independent and identically distributed (i.i.d) states and also non-i.i.d scenarios in the discrete-variable setting [58]. We

[4] See [51,54] for similar circuits.

assume that Alice has access to identical copies of Bob's resource state (the i.i.d setting). Our specific test relies on two ingredients. The first is to show a relationship between the fidelity between the final ideal and real m-mode states of Alice's computation and the fidelity between the ideal and real injected M-mode resource states. The second is to obtain a tight lower bound on the latter fidelity by means of a proper fidelity witness $\mathcal{W}$ using only Gaussian measurements, which Alice can perform. Finally, Alice's accept or reject decision is based on whether the value of the latter lower bound is high enough in comparison with the chosen threshold F_T.

We start with the first ingredient. We call the initial ideal state that Alice possesses (on both input and injected modes) $\sigma_{\text{in}} = |\Psi_{\text{in}}\rangle\langle\Psi_{\text{in}}| \otimes \sigma$, where $\sigma = (|\tilde{\gamma}\rangle_s\langle\tilde{\gamma}|_s)^{\otimes M}$ is the ideal resource state. The outcome of Alice's intended computation consists of an m-mode pure state (for each measurement outcome) that can be expressed as $\sigma_{\text{out}}(\mathbf{y}) = \mathcal{E}_{\mathbf{y}}(\sigma_{\text{in}})/\text{Tr}(\mathcal{E}_{\mathbf{y}}(\sigma_{\text{in}}))$. If Bob gives Alice ρ, her real initial state is $\rho_{\text{in}} = |\Psi_{\text{in}}\rangle\langle\Psi_{\text{in}}| \otimes \rho$ and her output state would be $\rho_{\text{out}}(\mathbf{y}) = \mathcal{E}_{\mathbf{y}}(\rho_{\text{in}})/\text{Tr}(\mathcal{E}_{\mathbf{y}}(\rho_{\text{in}}))$. Linearity of $\mathcal{E}_{\mathbf{y}}$ then implies the following lemma, proved in Appendix B.

Lemma 1. The fidelity between the final states $\sigma_{\text{out}}(\mathbf{y})$ and $\rho_{\text{out}}(\mathbf{y})$ satisfies the bound,

$$F(\sigma_{\text{out}}(\mathbf{y}), \rho_{\text{out}}(\mathbf{y})) \geqslant F(\sigma, \rho)\frac{\text{Tr}(\mathcal{E}_{\mathbf{y}}(\sigma_{\text{in}}))}{\text{Tr}(\mathcal{E}_{\mathbf{y}}(\rho_{\text{in}}))}. \tag{3}$$

Here we note that, in the case of finite squeezing, in general $\text{Tr}(\mathcal{E}_{\mathbf{y}}(\sigma_{\text{in}}))/\text{Tr}(\mathcal{E}_{\mathbf{y}}(\rho_{\text{in}})) \neq 1$. However, as we will see later from Theorem 2, this inequality is sufficient to imply ϵ verifiability independent of the amount of squeezing s.

We now focus on the second ingredient: efficient estimation the observable lower bound $F_{\text{low}} \equiv \text{Tr}(\mathcal{W}\rho)$ to the fidelity $F(\sigma, \rho)$ by measuring an adequate fidelity witness $\mathcal{W}$. A Hermitian observable $\mathcal{W}$ is a fidelity witness with respect to the target state σ if it has the properties that

$$F_{\text{low}} \equiv \text{Tr}(\mathcal{W}\rho) \leqslant F(\sigma, \rho), \tag{4}$$

for all ρ (universal lower bound) and $F_{\text{low}} = 1$ for $\rho = \sigma$ (tightness). Our specific witness is given by the following.

Lemma 2. The observable

$$\mathcal{W} = \left(1 + \frac{M}{2}\right)\mathbb{1}_M - \sum_{k=0}^{M-1} \mathbb{1}_k \otimes w_{k+1} \otimes \mathbb{1}_{M-k-1}, \tag{5}$$

is a fidelity witness with respect to the target state σ, where $w_{k+1} = (s^2/2)(\hat{x}_{k+1}^2 + 9\tilde{\gamma}^2\hat{x}_{k+1}^4) + (1/(2s^2))(\hat{p}_{k+1}^2 + 2\tilde{\gamma}\hat{p}_{k+1}^3) + (1/(2s^2))\tilde{\gamma}((\hat{x}_{k+1} - \hat{p}_{k+1})^3 - (\hat{x}_{k+1} + \hat{p}_{k+1})^3)$. Thus $\mathcal{W}$ is composed entirely of $O(M)$ terms accessible through Gaussian measurements alone [5].

Proof. See Appendix C. ■

Finally, we consider the accept or reject criterion of the verification test. A threshold fidelity $0 < F_T < 1$ and a significance level $0 < \beta < 1$ means that Alice must, with probability at least $1 - \beta$, reject the state ρ if $F(\sigma, \rho) < F_T$. To this end, the number N of copies of ρ she asks Bob for must be high enough for her to estimate F_{low} up to precision η and with failure probability at most β. In other words, the probability obeys $P(|F_{\text{low}}^{(\text{est})} - F_{\text{low}}| < \eta) \geqslant 1 - \beta$. With this, she then rejects whenever $F_{\text{low}}^{(\text{est})} < F_T + \eta$ and accepts otherwise. This guarantees the desired reject condition above. Conversely, if ρ is accepted (i.e., if $F_{\text{low}}^{(\text{est})} \geqslant F_T + \eta$), she knows that, with probability at least $1 - \beta$, that $F(\sigma, \rho) \geqslant F_T$.

The exact scaling of N with respect to M, η, and β defines the so-called *sample complexity* of the test, which depends on the specific measurement scheme chosen. Our method of directly estimating F_{low} is to use importance sampling techniques [53,59,60]. The basic idea of the importance sampling method is to choose the observables to measure probabilistically according to their importance for $\mathcal{W}$. The relative importance of each observable, given by the size of the coefficients λ_i, dictates the frequency with which it is measured, with less important observables measured less frequently. This optimizes the total number of measurements required.

We begin by inserting Eq. (5) into Eq. (4) to find $F_{\text{low}} = 1 + M/2 + \sum_{j=0}^{6M} \lambda_i \text{Tr}(\hat{f}_i\rho)$, where λ_i are coefficients depending only on s and $\tilde{\gamma}$ and $\hat{f}_i = \mathbb{1}_k \otimes \hat{x}'^{n}_{k+1} \otimes \mathbb{1}_{M-k-1}$, where $n = 1, 2, 3, 4$ and $\hat{x}' = \hat{x}, \hat{p}, \hat{x} \pm \hat{p}$ [6]. We can always rewrite $\hat{f}_i = \int df\, f \hat{P}_i$ where $f = (x'_{k+1})^n$, $\hat{P}_i = |x'_1, ..., x'_M\rangle\langle x'_1, ..., x'_M|$ is the projection onto quadratures $\hat{x}'_l$ in modes $l = 1, ..., M$, x'_{k+1} is the eigenvalue of the operator $\hat{f}_i$, and $df \equiv dx'_1...dx'_M$. We note that even though $\hat{f}_i$ are operators up to fourth order in the quadratures $\hat{x}'$, Gaussian measurements are sufficient to find the eigenvalues $f = (x'_{k+1})^n$ since the eigenvalues x'_{k+1} can be found by Gaussian projective measurements $\hat{P}_i$.

Then to estimate F_{low}, we can rewrite $\sum_{j=0}^{6M} \lambda_i \text{Tr}(\hat{f}_i\rho) = \sum_{j=0}^{6M} \int df\, p(i, f) F_{i,f} \equiv \langle\mathbf{F}\rangle$ where $\mathbf{F}$ is a random variable taking the value $F_{i,f} = \sum_{j=0}^{6M} |\lambda_j| \text{sgn}(\lambda_i) f$ with probability $p(i, f) = \text{Tr}(\hat{P}_i\rho)|\lambda_i|/\sum_{j=0}^{6M} |\lambda_j|$. See Appendix D for a derivation. To sample from $\mathbf{F}$, we begin by sampling the index i with probability $|\lambda_i|/(\sum_{j=0}^{6M} |\lambda_j|)$. Then given this i, we find the eigenvalue f corresponding to $\hat{f}_i$, which occurs with probability $\text{Tr}(\hat{P}_i\rho)$. From this f value, $F_{i,f}$ can be sampled with probability $p(i, f)$.

For the g^{th} sampling trial, where $g = 1, ..., N$, let the value of the corresponding $F_{i,f}$ be denoted $F^{(g)}$. For each g^{th} trial, a single copy of ρ is consumed. We can then obtain the estimate $F_{\text{low}}^{(\text{est})} = (1/N) \sum_{g=1}^{N} F^{(g)}$ by using N copies of ρ. In the limit $N \to \infty$, $F_{\text{low}}^{(\text{est})}$ will output the exact value F_{low}. With this method, we can obtain the following upper bound for N to certify our cubic phase state.

Lemma 3. Sampling complexity of the verification protocol.

[5] For example, homodyne detection in quantum optics is sufficient to achieve this. Here the expectation value of a linear function of $\hat{x}$, $\hat{p}$ is related to the expectation value of the photon number difference detected in the two arms of a homodyne detection setup. Thus higher powers of the expectation values of $\hat{x}$, $\hat{p}$ can be found by detecting the differences in the powers of the photon number operators. For example, see [69].

[6] For the exact coefficients see Appendix C.

If the number of copies of ρ used in our verification test satisfies

$$N \sim O\left(\frac{M^2}{\eta^2}\ln\left(\frac{1}{\beta}\right)\right), \tag{6}$$

then $P(|F_{\rm low}^{(\rm est)} - F_{\rm low}| < \eta) \geqslant 1-\beta$.

Proof. We use Hoeffding's inequality that leads to a sample complexity exponentially better in β compared to previous scalings based on Chebyshev's inequality [52]. For details of the proof see Appendix E. ■

This result provides an upper bound to the sample complexity of our verification test and relies on the physical assumption of finite energy available per mode of ρ. This also makes N efficient in the number of cubic phase states consumed by the computation.

Next, we shall show that our assisted protocol is ϵ verifiable, given the above results.

Theorem 2. Let N, η, β, and F_T be, respectively, the number of copies of the M-mode state ρ, the precision, the failure probability, and threshold fidelity used in Protocol 1. Assuming finite energy available per mode of ρ, our assisted protocol is ϵ verifiable, where $\epsilon = 1-(1-\beta)F_T$, where β and N are related by Lemma 3.

Proof. Our aim is to bound $\int d\mathbf{y}P(\text{incorrect} \cap \text{accept})P(\mathbf{y})$, which is the probability that Alice accepts ρ from Bob yet obtains an incorrect outcome to her computation. From Bayes' rule and $P(\text{accept}) \leqslant 1$, we have $P(\text{incorrect} \cap \text{accept}) = P(\text{incorrect}|\text{accept})P(\text{accept}) \leqslant P(\text{incorrect}|\text{accept})$. This means $\int d\mathbf{y}P(\text{incorrect} \cap \text{accept})P(\mathbf{y}) \leqslant \int d\mathbf{y}P(\text{incorrect}|\text{accept})P(\mathbf{y})$.

Thus, to show ϵ verifiability, it suffices to find an upper bound for the average conditional probability $\int d\mathbf{y} P(\text{incorrect}|\text{accept})P(\mathbf{y}) = \int d\mathbf{y}\text{Tr}(\Pi_{\text{incorrect}}\rho_{\text{out}}(\mathbf{y}))P(\mathbf{y})$, where $\text{Tr}(\Pi_{\text{incorrect}}\rho_{\text{out}}(\mathbf{y})) = 1-\text{Tr}(\sigma_{\text{out}}(\mathbf{y})\rho_{\text{out}}(\mathbf{y})) = 1-F(\sigma_{\text{out}}(\mathbf{y}), \rho_{\text{out}}(\mathbf{y}))$, $\rho_{\text{out}}(\mathbf{y}) = \mathcal{E}_{\mathbf{y}}(|\Psi_{\text{in}}\rangle\rangle\Psi_{\text{in}}| \otimes \rho)$, and $P(\mathbf{y}) = P(\rho_{\text{out}}(\mathbf{y}))$ if Alice accepts ρ.

Suppose $\sigma_{\text{out}}(\mathbf{y}) = \mathcal{E}_{\mathbf{y}}(\sigma_{\text{in}})/\text{Tr}(\mathcal{E}_{\mathbf{y}}(\sigma_{\text{in}}))$ is the output state of Alice's circuit (with honest Bob) which includes projective measurements. For finite squeezing this would also depend on measurement results $\mathbf{y}$. This is a pure state, so we can write

$$\begin{aligned} P(\text{incorrect}|\text{accept}) &= \frac{\text{Tr}((\mathbf{1}_m - \sigma_{\text{out}}(\mathbf{y})))(\mathcal{E}_{\mathbf{y}}(\rho_{\text{in}}))}{\text{Tr}(\mathcal{E}_{\mathbf{y}}(\rho_{\text{in}}))} \\ &= \text{Tr}((\mathbf{1}_m - \sigma_{\text{out}}(\mathbf{y}))\rho_{\text{out}}(\mathbf{y})). \end{aligned} \tag{7}$$

This means $\int d\mathbf{y}P(\text{incorrect}|\text{accept})P(\mathbf{y}) = 1 - \int d\mathbf{y}\text{Tr}(\sigma_{\text{out}}(\mathbf{y})\rho_{\text{out}}(\mathbf{y}))P(\mathbf{y})$, where $P(\mathbf{y}) = \text{Tr}(\mathcal{E}_{\mathbf{y}}(\rho_{\text{in}}))$ is the probability of Alice's outcome state having measurement outcomes $\mathbf{y}$ if Alice accepts ρ_{in}.

We can now show the upper bound $\int d\mathbf{y}P(\text{incorrect}|\text{accept}) \leqslant \epsilon$ to demonstrate that our scheme is ϵ verifiable, where $\epsilon = 1-(1-\beta)F_T$.

The first step is to compute $P(\text{incorrect}|\text{accept}, \mathbf{y})$ by expanding the RHS of Eq. (7),

$$P(\text{incorrect}|\text{accept}) = 1 - \mathcal{F}(\sigma_{\text{out}}(\mathbf{y}), \rho_{\text{out}}(\mathbf{y})). \tag{8}$$

In our Lemma 1, we showed that, without any extra assumptions, the fidelity between the final states $\sigma_{\text{out}}(\mathbf{y})$ and $\rho_{\text{out}}(\mathbf{y})$ satisfies the bound $F(\sigma_{\text{out}}(\mathbf{y}), \rho_{\text{out}}(\mathbf{y})) \geqslant F(\sigma, \rho)\text{Tr}(\mathcal{E}_{\mathbf{y}}(\sigma_{\text{in}}))/\text{Tr}(\mathcal{E}_{\mathbf{y}}(\rho_{\text{in}})$. To simplify notation, we can write $\text{Tr}(\mathcal{E}_{\mathbf{y}}(\sigma_{\text{in}})) = p_{\mathbf{y}}(\sigma_{\text{in}})$ and $\text{Tr}(\mathcal{E}_{\mathbf{y}}(\rho_{\text{in}})) = P(\mathbf{y})$ which correspond to the probabilities of the final states of the device giving measurement results $\mathbf{y}$ for input states σ_{in} and ρ_{in}, respectively. Then inserting Lemma 1 into Eq. (8) we arrive at $P(\text{incorrect}|\text{accept}) \leqslant 1 - \mathcal{F}(\sigma, \rho)p_{\mathbf{y}}(\sigma_{\text{in}})/P(\mathbf{y})$, which means

$$\begin{aligned} &\int d\mathbf{y}P(\text{incorrect}|\text{accept})P(\mathbf{y}) \\ &\leqslant \int d\mathbf{y}\left(1 - \mathcal{F}(\sigma, \rho)\frac{p_{\mathbf{y}}(\sigma_{\text{in}})}{P(\mathbf{y})}\right)P(\mathbf{y}) \\ &= 1 - \mathcal{F}(\sigma, \rho), \end{aligned} \tag{9}$$

since $\int d\mathbf{y}p_{\mathbf{y}}(\sigma_{\text{in}}) = 1$. Alice's accept condition implies that $F(\sigma, \rho) \geqslant F_T$ with probability at least $1-\beta$. This means we can now write $\rho = (1-\beta')(F'\sigma + (1-F')\sigma_\perp) + \beta'\sigma'$, where $F' \geqslant F_T$, $\beta' \leqslant \beta$, $\text{Tr}(\sigma\sigma_\perp) = 0$, and σ' is a quantum state. This implies $F(\sigma, \rho) = \text{Tr}(\sigma\rho) \geqslant (1-\beta')F' \geqslant (1-\beta)F_T$. Thus from Eq. (9), we have

$$\int d\mathbf{y}P(\text{incorrect}|\text{accept})P(\mathbf{y}) \leqslant 1-(1-\beta)F_T.$$

Choosing $\epsilon = 1-(1-\beta)F_T$ gives us the bound we need. This is true for finite squeezing as well as infinite squeezing. ■

IV. DISCUSSION

As a final remark, it is important to point out that the i.i.d assumption for Bob's state preparation can actually be removed. This relies on Serfling's bound, which is an improvement over Hoeffding's bound as it does not require the i.i.d assumption (it considers sampling without replacement) [61]. CV stabilizer states can be verified using a binary-outcome test based on the fact that they are extremal on stabilizer operators [62]. Since such a test defines a two-dimensional random variable, it can be handled with Serfling's bound. Remarkably, a similar test can be designed for the single-mode cubic phase state, as it is extremal on the fidelity witness $\mathcal{W} = 3/2 - w$ introduced in Eq. (5). More precisely, the cubic phase state is, by construction, a unique eigenstate of $\mathcal{W}$ with (maximal) eigenvalue 1. This allows us to safely relax the i.i.d assumption. We leave the details of this fascinating prospect for future work.

ACKNOWLEDGMENTS

The authors acknowledge support from the Singapore National Research Foundation under NRF Award No. NRF-NRFF2013-01, ANR-NRF Grant No. NRF2017-NRF-ANR004, and the U.S. Air Force Office of Scientific Research under AOARD Grant No. FA2386-15-1-4082. L.A. acknowledges financial support from the Brazilian agencies CNPq (PQ Grant No. 311416/2015-2 and INCT-IQ), FAPERJ (JCN E- 26/202.701/2018), CAPES (PROCAD2013), INCT-IQ (National Institute for Science and Technology of Quantum Information), and the Serrapilheira Institute (Grant No. Serra-1709-17173). The authors would like to thank Renato M. S. Farias and an anonymous referee for helpful comments on the manuscript, and also Atul Mantri for interesting and valuable discussions about the concepts of blindness and verification.

APPENDIX A: GATE TELEPORTATION PROTOCOL FOR THE CUBIC PHASE GATE

We begin with the circuit in Fig. 2 with initial state $(\mathbb{1}_{m-1}\otimes S(r)\otimes \mathbb{1})|\Psi\rangle_{\text{in}}\otimes|\tilde{\gamma}\rangle_s$, where we choose $k=m-1$ here for simplicity. The results generalize easily for any other $k=0,..,m$. Let $\mathbf{x}=(x_1,\dots,x_m)$. We can write the m-mode state as $|\Psi_{\text{in}}\rangle=\int d^n\mathbf{x}\psi(\mathbf{x})|\mathbf{x}\rangle$, for some bounded function $\psi(\mathbf{x})$, then $(\mathbb{1}_{m-1}\otimes S(r))|\Psi_{\text{in}}\rangle=\int d^m\mathbf{x}\psi_r(\mathbf{x})|\mathbf{x}\rangle$. We apply the control operator $\mathbb{1}_{m-1}\otimes\exp(i\hat{x}\otimes\hat{p})$ on the initial state, and measure $\hat{x}$ in the last register with outcome $\mathbf{y}$. The final state becomes

$$|\Psi\rangle_s\otimes|\mathbf{y}\rangle \tag{A1}$$

$$\begin{aligned}
&=(\mathbb{1}_m\otimes|\mathbf{y}\rangle\langle\mathbf{y}|)(\mathbb{1}_{m-1}\otimes e^{i\hat{x}\otimes\hat{p}})\\
&\quad\times(\mathbb{1}_{m-1}\otimes S(r)\otimes\mathbb{1})(|\Psi_{\text{in}}\rangle\otimes|\tilde{\gamma}\rangle_s)\\
&=\frac{\mathbb{1}_m\otimes|\mathbf{y}\rangle\langle\mathbf{y}|}{\sqrt{s}\pi^{1/4}}(\mathbb{1}_{m-1}\otimes e^{i\hat{x}\otimes\hat{p}})\int d^m\mathbf{x}\int dx\psi_r(\mathbf{x})\\
&\quad\times e^{i\tilde{\gamma}x^3}e^{-x^2/(2s^2)}|\mathbf{x},x\rangle\\
&=\frac{\mathbb{1}_m\otimes|\mathbf{y}\rangle\langle\mathbf{y}|}{\sqrt{s}\pi^{1/4}}(\mathbb{1}_m\otimes e^{ix_m\hat{p}})\int d^m\mathbf{x}\int x\psi_r(\mathbf{x})\\
&\quad\times e^{i\tilde{\gamma}x^3}e^{-x^2/(2s^2)}|\mathbf{x},x\rangle\\
&=\frac{\mathbb{1}_m\otimes|\mathbf{y}\rangle\langle\mathbf{y}|}{\sqrt{s}\pi^{1/4}}\int d^m\mathbf{x}\int dxe^{i\tilde{\gamma}x^3}e^{-x^2/(2s^2)}\psi_r(\mathbf{x})\\
&\quad\times|\mathbf{x},x-x_m\rangle\\
&=\frac{(\mathbb{1}_{m-1}\otimes G(\mathbf{y})e^{i\tilde{\gamma}\hat{x}^3}g_s(\mathbf{y})S(r)\otimes\mathbb{1})|\Psi_{\text{in}}\rangle\otimes|\mathbf{y}\rangle}{\sqrt{s}\pi^{1/4}},
\end{aligned}\tag{A2}$$

where $G(\mathbf{y})\equiv\exp(i\tilde{\gamma}\mathbf{y}^3)\exp(3i\tilde{\gamma}\mathbf{y}\hat{x}(\mathbf{y}+\hat{x}))$ is a unitary Gaussian correction in the operator $\hat{x}$, and $g_s(\mathbf{y})=\exp(-(\hat{x}+\mathbf{y})^2/(2s^2))$ is a smearing operation that applies a Gaussian envelope, with width $\sim 1/s^2$ centered on $\mathbf{y}$, onto the state it acts upon.

Using $S^\dagger(r)\hat{x}S(r)=r\hat{x}$, we can rewrite the above state as $|\Psi\rangle_s=G(\mathbf{y})e^{i\tilde{\gamma}\hat{x}^3}S(r)|\tilde{\Psi}_{\text{in}}\rangle$, where $|\tilde{\Psi}_{\text{in}}\rangle=g_{s/r}(\mathbf{y}/r)|\Psi_{\text{in}}\rangle$ is now a Gaussian-smeared state where the Gaussian envelope has width $\sim s/r$ centered on $\mathbf{y}/r$. Note that this Gaussian envelope is of the same type that appears in the usual CV cluster state computation [63].

Then Alice applies a unitary Gaussian $\mathbb{1}^{\otimes(m-1)}\otimes S^\dagger(r)G^{-1}(\mathbf{y})$ onto $|\Psi\rangle_s$ to obtain

$$|\Psi_{\text{out}}(\mathbf{y})\rangle_s=e^{i\gamma\hat{x}^3}g_{s/r}(\mathbf{y}/r)|\Psi_{\text{in}}\rangle, \tag{A3}$$

where $r=(\gamma/\tilde{\gamma})^{1/3}$.

Note that in the infinite squeezing $s\to\infty$ limit, we obtain the exact cubic phase gate operation $|\Psi_{\text{out}}\rangle_{s\to\infty}=e^{i\gamma\hat{x}^3}|\Psi_{\text{in}}\rangle$ which is independent of $\mathbf{y}$.

Instead of the teleportation circuit in Fig. 2, it is also possible to use either the passive linear optics circuit in [46] or an alternative circuit in [64], which both have as inputs cubic phase states as the non-Gaussian resource state. Since our results only depend on having stand-alone cubic phase states and Gaussian channels, our main results equally apply for these circuits, too.

To clarify, for the finite squeezing scenario, the ideal outcome is defined in Eq. (A3), which depends on measurement outcomes. This in turn means that P(incorrect), which is related to one minus the overlap between the actual and ideal outcome, is generally not zero even if the probability of getting a particular homodyne measurement outcome has measure zero. The case is even simpler in the infinite squeezing limit where the ideal outcome does not depend on measurement outcomes at all.

We note that in continuous-variable quantum computation it is possible for finite squeezing effects to limit the effective length of the computation (e.g., see [65]), depending on the amount of squeezing available. This is an important issue concerning all continuous-variable schemes, certainly worth future investigations, but it is outside the scope of this current work.

Finally, we know that currently a high amount of squeezing may not be necessarily easier to experimentally achieve compared to non-Gaussian resources like single-photon states and photon-number resolving detection. However, we do not consider the latter non-Gaussian resources, as it is not obvious how to design simple gates with them [54].

APPENDIX B: PROOF OF LEMMA 1

First, we show that, for any mixed state ρ_{in} and any pure state σ_{in}, there exists a density matrix $\sigma^\perp$ such that

$$\rho_{\text{in}}=F(\sigma_{\text{in}},\rho_{\text{in}})\sigma_{\text{in}}+(1-F(\sigma_{\text{in}},\rho_{\text{in}}))\sigma^\perp, \tag{B1}$$

and $F(\sigma^\perp,\sigma_{\text{in}})=0$. In our delegation protocol, σ_{in} is an $m+M$-mode state $|\Psi_{\text{in}}\rangle\langle\Psi_{\text{in}}|\otimes\sigma$, where σ is a pure M-mode product state. Given that $F(\sigma_{\text{in}},\rho_{\text{in}})=\text{Tr}(\sigma_{\text{in}}\rho_{\text{in}})$, we can interpret this fidelity to be the projection of ρ_{in} onto the subspace spanned by σ_{in}. This is because the trace of the product of two matrices is a valid Hilbert-Schmidt inner product. All the other components of ρ_{in} must be in the orthogonal subspace to σ_{in}, $\sigma^\perp$. Thus Eq. (B1) must hold while satisfying $F(\sigma^\perp,\sigma_{\text{in}})=0$.

Next, we demonstrate $\sigma^\perp$ is a valid density matrix. There are two requirements: $\text{Tr}(\sigma^\perp)=1$, and $\sigma^\perp$ is positive semidefinite. The first condition follows directly by taking the trace on both sides of Eq. (B1). To show the latter, we rewrite $\sigma^\perp=O\rho_{\text{in}}O^\dagger$, where $O=(\mathbb{1}_{m+M}-\sigma_{\text{in}})/\sqrt{1-F(\sigma_{\text{in}},\rho_{\text{in}})}$, which we note satisfies the requisite $\text{Tr}(\sigma_{\text{in}}\sigma^\perp)=0$. Since ρ_{in} is positive semidefinite, it can be written as $\rho_{\text{in}}=A^\dagger A$, for some matrix A. Thus $\sigma^\perp$ is also positive semidefinite because we can write $\sigma^\perp=(AO^\dagger)^\dagger(AO^\dagger)$.

Recall that $\sigma_{\text{in}}=|\Psi_{\text{in}}\rangle\langle\Psi_{\text{in}}|\otimes\sigma$, where σ is a pure state, and the actual initial state to be tested is $\rho_{\text{in}}=|\Psi_{\text{in}}\rangle\langle\Psi_{\text{in}}|\otimes\rho$, where ρ is in general a mixed state. Then, using these in Eq. (B1) gives us

$$\rho_{\text{in}}=F(\sigma,\rho)\sigma_{\text{in}}+(1-F(\sigma,\rho))\sigma^\perp, \tag{B2}$$

where $F(\sigma_{\text{in}},\sigma^\perp)=0$. Applying the linear operator $\mathcal{E}_{\mathbf{y}}$ that represents the teleportation circuit to Eq. (B2),

$$\mathcal{E}_{\mathbf{y}}(\rho_{\text{in}})=F(\sigma,\rho)\mathcal{E}_{\mathbf{y}}(\sigma_{\text{in}})+(1-F(\sigma,\rho))\mathcal{E}_{\mathbf{y}}(\sigma^\perp). \tag{B3}$$

Since $\sigma_{\text{out}}(\mathbf{y})$ is a pure state (where in the case of performing a single cubic gate $\sigma_{\text{out}}(\mathbf{y})=|\Psi_{\text{out}}(\mathbf{y})\rangle_s\langle\Psi_{\text{out}}(\mathbf{y})|_s$), we can write the fidelity between $\sigma_{\text{out}}(\mathbf{y})$ and $\rho_{\text{out}}(\mathbf{y})$ as

$$F(\sigma_{\text{out}}(\mathbf{y}), \rho_{\text{out}}(\mathbf{y})) = \text{Tr}(\sigma_{\text{out}}(\mathbf{y})\rho_{\text{out}}(\mathbf{y})). \tag{B4}$$

The fidelity between the final states $\sigma_{\text{out}}(\mathbf{y})$ and $\rho_{\text{out}}(\mathbf{y})$ then satisfies the bound,

$$\begin{aligned} &F(\sigma_{\text{out}}(\mathbf{y}), \rho_{\text{out}}(\mathbf{y})) \\ &= \frac{\text{Tr}(\mathcal{E}_{\mathbf{y}}(\sigma_{\text{in}})\mathcal{E}_{\mathbf{y}}(\rho_{\text{in}}))}{\text{Tr}(\mathcal{E}_{\mathbf{y}}(\sigma_{\text{in}}))\text{Tr}(\mathcal{E}_{\mathbf{y}}(\rho_{\text{in}}))} \\ &= \frac{F(\sigma,\rho)\text{Tr}(\mathcal{E}_{\mathbf{y}}(\sigma_{\text{in}})^2)+(1-F(\sigma,\rho))\text{Tr}(\mathcal{E}_{\mathbf{y}}(\sigma_{\text{in}})\mathcal{E}_{\mathbf{y}}(\sigma^{\perp}))}{\text{Tr}(\mathcal{E}_{\mathbf{y}}(\sigma_{\text{in}}))\text{Tr}(\mathcal{E}_{\mathbf{y}}(\rho_{\text{in}}))} \\ &\geqslant F(\sigma,\rho)\frac{\text{Tr}(\mathcal{E}_{\mathbf{y}}(\sigma_{\text{in}})^2)}{\text{Tr}(\mathcal{E}_{\mathbf{y}}(\sigma_{\text{in}}))\text{Tr}(\mathcal{E}_{\mathbf{y}}(\rho_{\text{in}}))} = F(\sigma,\rho)\frac{\text{Tr}(\mathcal{E}_{\mathbf{y}}(\sigma_{\text{in}}))}{\text{Tr}(\mathcal{E}_{\mathbf{y}}(\rho_{\text{in}}))}. \end{aligned} \tag{B5}$$

In the third line we used the fact that $1 - F(\sigma,\rho) \geqslant 0$ and $\text{Tr}(\mathcal{E}_{\mathbf{y}}(\sigma_{\text{in}})\mathcal{E}_{\mathbf{y}}(\sigma^{\perp})) \geqslant 0$ and $\mathcal{E}_{\mathbf{y}}(\sigma^{\perp})$ is positive semidefinite. In the last equality we used the fact that $\mathcal{E}_{\mathbf{y}}(\sigma_{\text{in}})/\text{Tr}(\mathcal{E}_{\mathbf{y}}(\sigma_{\text{in}}))$ is a pure normalized state, so $\text{Tr}(\mathcal{E}_{\mathbf{y}}(\sigma_{\text{in}})^2)/(\text{Tr}(\mathcal{E}_{\mathbf{y}}(\sigma_{\text{in}})))^2 = 1$. Note that in the infinite squeezing limit we have $\text{Tr}(\mathcal{E}_{\mathbf{y}}(\sigma_{\text{in}})) = \text{Tr}(\mathcal{E}_{\mathbf{y}}(\rho_{\text{in}}))$, so $F(\sigma_{\text{out}}(\mathbf{y}), \rho_{\text{out}}(\mathbf{y})) \geqslant \mathcal{F}(\sigma,\rho)$.

APPENDIX C: DERIVING F_{low}

We can write our ideal M-mode resource state as $\sigma = (|\tilde{\gamma}\rangle_s\langle\tilde{\gamma}|_s)^{\otimes M} = V^{\otimes M}|0\rangle_M\langle 0|_M(V^{\dagger})^{\otimes M}$, where $V = C(\tilde{\gamma})S(s)$ and $|0\rangle_M$ is the M-mode vacuum state. This means we can rewrite the squared quantum fidelity as

$$F(\sigma,\rho) = \text{Tr}(\sigma\rho) = \text{Tr}(|0\rangle_M\langle 0|_M((V^{\dagger})^{\otimes M}\rho V^{\otimes M})). \tag{C1}$$

To find a lower bound to this quantity, we first note that

$$|0\rangle_M\langle 0|_M \geqslant \mathbb{1}_M - \sum_{k=0}^{M-1}\mathbb{1}_k \otimes \hat{n}_{k+1} \otimes \mathbb{1}_{M-k-1}, \tag{C2}$$

where $\hat{n}_k$ is the number operator acting on the k^{th} mode. We can see this inequality by acting the left- and right-hand sides with the Fock states $|n_1, ..., n_M\rangle$, where $n_1, ..., n_M$ are non-negative integers. These Fock states form a complete eigenbasis. When using the Fock state $|0\rangle_M$, the inequality above becomes an equality. Otherwise, the inequality implies $0 \geqslant 1 - (n_1 + ... + n_M)$, which always holds.

Since $(V^{\dagger})^{\otimes M}\rho V^{\otimes M}$ is positive semidefinite, then Eqs. (C1) and (C2) give the lower bound to the fidelity,

$$F(\sigma,\rho) \geqslant \text{Tr}(\mathcal{W}\rho) \equiv F_{\text{low}}, \tag{C3}$$

where the fidelity witness $\mathcal{W}$ is

$$\mathcal{W} = \mathbb{1}_M - \sum_{k=0}^{M-1}\mathbb{1}_k \otimes V^{\dagger}\hat{n}_{k+1}V \otimes \mathbb{1}_{M-k-1}. \tag{C4}$$

The implication of this simple relation is that by writing $V\hat{n}V^{\dagger}$ in terms of $\hat{x}$ and $\hat{p}$, we can find a lower bound on fidelity by just measuring those quadratures of a given state ρ to find how close it is to our true cubic phase state. Note that this is a tight bound. This means if $\sigma = \rho$, then $F = 1 = F_{\text{low}}$.

To compute F_{low}, we find $V\hat{n}V^{\dagger}$ in terms of $\hat{x}$ and $\hat{p}$ by first using

$$\begin{aligned} S(s)\hat{n}S(s)^{\dagger} = a^{\dagger}a(2\cosh^2(\log(s)) - 1) \\ + \cosh(\log(s))\sinh(\log(s))(a^{\dagger}a^{\dagger} + aa) \\ + \sinh^2(\log(s))\mathbb{1}, \end{aligned} \tag{C5}$$

where number operator $\hat{n} = a^{\dagger}a$ can be defined in terms of the creation and annihilation operators $a^{\dagger} = (1/\sqrt{2})(\hat{x} - i\hat{p})$ and $a = (1/\sqrt{2})(\hat{x} + i\hat{p})$, respectively. By also using $\exp(i\tilde{\gamma}\hat{x}^3)a^{\dagger}\exp(-i\tilde{\gamma}\hat{x}^3) = (\exp(i\tilde{\gamma}\hat{x}^3)a\exp(-i\tilde{\gamma}\hat{x}^3))^{\dagger} = (1/\sqrt{2})(\hat{x} + 3i\tilde{\gamma}\hat{x}^2 - i\hat{p})$, we find

$$\begin{aligned} V\hat{n}V^{\dagger} &= -\frac{1}{2}\mathbb{1} + \frac{s^2}{2}(\hat{x}^2 + 9\tilde{\gamma}^2\hat{x}^4) + \frac{1}{2s^2}(\hat{p}^2 - 6\tilde{\gamma}\hat{x}\hat{p}\hat{x}) \\ &= -\frac{1}{2}\mathbb{1} + \frac{s^2}{2}(\hat{x}^2 + 9\tilde{\gamma}^2\hat{x}^4) + \frac{1}{2s^2}(\hat{p}^2 + 2\tilde{\gamma}\hat{p}^3) \\ &\quad + \frac{1}{2s^2}\tilde{\gamma}((\hat{x} - \hat{p})^3 - (\hat{x} + \hat{p})^3), \end{aligned} \tag{C6}$$

where we used $2\hat{x}\hat{p}\hat{x} = \hat{p}\hat{x}^2 + \hat{x}^2\hat{p}$ in the first line. Inserting Eq. (C6) into Eq. (C4) we can write

$$\mathcal{W} = \left(1 + \frac{M}{2}\right)\mathbb{1}_M - \sum_{k=0}^{M-1}\mathbb{1}_k \otimes w_{k+1} \otimes \mathbb{1}_{M-k-1}, \tag{C7}$$

where $w_{k+1} = (s^2/2)(\hat{x}_{k+1}^2 + 9\tilde{\gamma}^2\hat{x}_{k+1}^4) + (1/(2s^2))(\hat{p}_{k+1}^2 + 2\tilde{\gamma}\hat{p}_{k+1}^3) + (1/(2s^2))\tilde{\gamma}((\hat{x}_{k+1} - \hat{p}_{k+1})^3 - (\hat{x}_{k+1} + \hat{p}_{k+1})^3)$. Then we can write F_{low} as the sum,

$$F_{\text{low}} = 1 + \frac{M}{2} + \sum_{i=0}^{6M}\lambda_i\text{Tr}(\hat{f}_i\rho), \tag{C8}$$

where λ_i are real coefficients and $\hat{f}_i$ are tensor products of quadrature operators with unit coefficients obtained by inserting Eq. (C6) into Eqs. (C3) and (C4). Thus $\lambda_{1+6k} = -s^2/2$, $\lambda_{2+6k} = -9\tilde{\gamma}^2s^2/2$, $\lambda_{3+6k} = -1/(2s^2)$, $\lambda_{4+6k} = -\tilde{\gamma}/s^2$, $\lambda_{5+6k} = -\tilde{\gamma}/(2s^2)$, $\lambda_{6+6k} = \tilde{\gamma}/(2s^2)$, and $\hat{f}_{1+6k} = \mathbb{1}_k \otimes \hat{x}_{k+1} \otimes \mathbb{1}_{M-k-1}$, $\hat{f}_{2+6k} = \mathbb{1}_k \otimes \hat{x}_{k+1}^4 \otimes \mathbb{1}_{M-k-1}$, $\hat{f}_{3+6k} = \mathbb{1}_k \otimes \hat{p}_{k+1}^2 \otimes \mathbb{1}_{M-k-1}$, $\hat{f}_{4+6k} = \mathbb{1}_k \otimes \hat{p}_{k+1}^3 \otimes \mathbb{1}_{M-k-1}$, $\hat{f}_{5+6k} = \mathbb{1}_k \otimes (\hat{x}_{k+1} - \hat{p}_{k+1})^3 \otimes \mathbb{1}_{M-k-1}$, $\hat{f}_{5+6k} = \mathbb{1}_k \otimes (\hat{x}_{k+1} + \hat{p}_{k+1})^3 \otimes \mathbb{1}_{M-k-1}$, where $k = 0, 1, 2, ...$ with a maximum value of $M - 1$.

We note that state certification can also be achieved using state tomography by implementing homodyne detection [66,67]. However, this requires homodyning all (in principle infinitely many) quadratures instead of just four of them per mode as in our method here.

APPENDIX D: IMPORTANCE SAMPLING METHOD

Here we include more details on how F_{low} can be estimated using importance sampling techniques [53,59,60].

From Eq. (C8) we defined $F_{\text{low}} = 1 + M/2 + \sum_{i=0}^{6M}\lambda_i\text{Tr}(\hat{f}_i\rho)$ and $\hat{f}_i = \mathbb{1}_k \otimes \hat{x}_{k+1}^{\prime n} \otimes \mathbb{1}_{M-k-1}$, where $n = 1, 2, 3, 4$ and $\hat{x}' = \hat{x}, \hat{p}, \hat{x} \pm \hat{p}$. Since M is known, we only need to estimate the quantity $\sum_{i=0}^{6M}\lambda_i\text{Tr}(\hat{f}_i\rho)$. We then define a random variable $\mathbf{F}$ which takes the values $F_{i,f} \equiv \sum_{j=0}^{6M}|\lambda_j|\text{sgn}(\lambda_i)f$, where f are the eigenvalues of the quadrature operators $\hat{f}_i = \int df f \hat{P}_i$, where $f = (x'_{k+1})^n$, $P_i = |x'_1, ..., x'_M\rangle\langle x'_1, ..., x'_M|$ is the projection onto quadratures $\hat{x}'_l$ in modes $l = 1, ..., M$, x'_{k+1} is the eigenvalue of the operator $\hat{f}_i$, and $df \equiv dx'_1...dx'_M$.

We can also define a probability density $p(i, f) = p(i)p(f|i)$ for $\mathbf{F}$, where $p(i) = |\lambda_i|/\sum_{j=0}^{6M}|\lambda_j|$. The conditional probability term $p(f|i) = \mathrm{Tr}(\hat{P}_i\rho)$. This means we can rewrite $F_{\text{low}} - 1 - M/2 = \sum_{i=0}^{6M}\int df\, p(i, f)F_{i,f}$, which we show below,

$$
\begin{aligned}
&F_{\text{low}} - 1 - M/2\\
&\quad = \sum_{i=0}^{6M}\lambda_i \mathrm{Tr}(\hat{f}_i\rho)\\
&\quad = \sum_{i=0}^{6M}\frac{|\lambda_i|}{\sum_{j=0}^{6M}|\lambda_j|}\mathrm{Tr}\left(\mathrm{sgn}(\lambda_i)\sum_{k=0}^{6M}|\lambda_k|\hat{f}_i\rho\right)\\
&\quad = \sum_{i=0}^{6M}\frac{|\lambda_i|}{\sum_{j=0}^{6M}|\lambda_j|}\mathrm{Tr}\left(\mathrm{sgn}(\lambda_i)\sum_{k=0}^{6M}|\lambda_k|\int df f\hat{P}_{i,f}\rho\right)\\
&\quad = \sum_{i=0}^{6M}\int df\frac{|\lambda_i|}{\sum_{j=0}^{6M}|\lambda_j|}\mathrm{Tr}(\hat{P}_{i,f}\rho)\sum_{k=0}^{6M}|\lambda_k|\mathrm{sgn}(\lambda_i)f\\
&\quad = \sum_{i=0}^{6M}\int df\, p(i, f)F_{i,f} \equiv \langle\mathbf{F}\rangle.
\end{aligned}
\tag{D1}
$$

In this way, we can consider F_{low} as the expectation value of the random variable $\mathbf{F}$ which takes on the values $F_{i,f}$ with probability $p(i, f)$.

APPENDIX E: SAMPLE COMPLEXITY

We know from Appendix D that $\mathbf{F}$ is a random variable which takes value $F_{i,f}$ with probability $p(i, f)$. Due to finite energy constraints in real experiments, this variable is always bounded in the interval $[\min F_{i,f}, \max F_{i,f}]$. Then from Hoeffding's inequality, if we sample $F_{i,f}$ values N times, the probability $|F^{(\text{est})}_{\text{low}} - F_{\text{low}}| \geqslant \eta$ is upper bounded by

$$
P\left(\left|F^{(\text{est})}_{\text{low}} - F_{\text{low}}\right| \geqslant \eta\right) \leqslant e^{-2N\eta^2/(\min F_{i,f}-\max F_{i,f})^2}. \tag{E1}
$$

Thus the minimal number of copies of ρ required to ensure $P(|F^{(\text{est})}_{\text{low}} - F_{\text{low}}| < \eta) \geqslant 1 - \beta$ is $N \sim O(\ln(1/\beta)(\min F_{i,f} - \max F_{i,f})^2/\eta^2)$. In the following, we derive the upper bound to $(\min F_{i,f} - \max F_{i,f})^2 \leqslant KM^2$, where K is a bounded constant independent of M.

From Appendix D we know we can write $F_{i,f} = \sum_{j=0}^{6M}|\lambda_j|\mathrm{sgn}(\lambda_i)f$, which means $\max F_{i,f} \leqslant \sum_{j=0}^{6M}|\lambda_j||f| \leqslant 6M\max(|\lambda_j|)\max(|f|)$ and $\min F_{i,f} \geqslant -6M\max(|\lambda_j|)\max(|f|)$. Thus

$$
(\min F_{i,f} - \max F_{i,f})^2 \leqslant 4(6M)^2\max(|\lambda_j|)^2\max(|f|)^2. \tag{E2}
$$

We note that λ_j depends only on the squeezing s and $\tilde{\gamma}$ and under physical assumptions of finite energy available to Alice and Bob, $|\lambda_j|$ is bounded from above and is independent of M. Also, $\hat{f}_j$ are all local quadrature operators polynomial in $\hat{x}$ and $\hat{p}$ up to order 4. Since the operators are local, the maximum values of $|f|$ do not depend on M and can be related to an upper bound of the energy of ρ per mode when the quadrature operators are quadratic. Otherwise, we can assume finite upper bounds of the higher moments of the quadrature operators. So $(\min F_{i,f} - \max F_{i,f})^2 \leqslant KM^2$, where K is a bounded constant independent of M. Therefore, if

$$
N \sim \mathcal{O}\left(\frac{M^2}{\eta^2}\ln\left(\frac{1}{\beta}\right)\right), \tag{E3}
$$

then $P(|F^{(\text{est})}_{\text{low}} - F_{\text{low}}| < \eta) \geqslant 1 - \beta$.

[1] S. Lloyd, Universal quantum simulators, Science **273**, 1073 (1996).

[2] J. I. Cirac and P. Zoller, Goals and opportunities in quantum simulation, Nat. Phys. **8**, 264 (2012).

[3] I. M. Georgescu, S. Ashhab, and F. Nori, Quantum simulation, Rev. Mod. Phys. **86**, 153 (2014).

[4] L. K. Grover, Quantum Mechanics Helps in Searching for a Needle in a Haystack, Phys. Rev. Lett. **79**, 325 (1997).

[5] A. W. Harrow, A. Hassidim, and S. Lloyd, Quantum Algorithm for Linear Systems of Equations, Phys. Rev. Lett. **103**, 150502 (2009).

[6] N. Wiebe, D. Braun, and S. Lloyd, Quantum Algorithm for Data Fitting, Phys. Rev. Lett. **109**, 050505 (2012).

[7] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, Quantum machine learning, Nature (London) **549**, 195 (2017).

[8] V. Dunjko and H. J. Briegel, Machine learning & artificial intelligence in the quantum domain, Rep. Prog. Phys. **81**, 074001 (2018).

[9] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM Rev. **41**, 303 (1999).

[10] B. P. Lanyon, T. J. Weinhold, N. K. Langford, M. Barbieri, D. F. V. James, A. Gilchrist, and A. G. White, Experimental Demonstration of a Compiled Version of Shor's Algorithm with Quantum Entanglement, Phys. Rev. Lett. **99**, 250505 (2007).

[11] J. Fitzsimons, Private quantum computation: An introduction to blind quantum computing and related protocols, npj Quantum Inf. **3**, 23 (2017).

[12] A. Childs, Secure assisted quantum computation, Quantum Inf. Comput. **5**, 456 (2005).

[13] D. Aharonov, M. Ben-Or, and E. Eban, Interactive proofs for quantum computations, in *Proceeding of Innovations in Computer Science 2010* (ICS, Beijing, 2010), pp. 453–469.

[14] A. Broadbent, J. Fitzsimons, and E. Kashefi, Universal blind quantum computation, in *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS)* (IEEE, Piscataway, 2009), pp. 517–526.

[15] J. F. Fitzsimons and E. Kashefi, Unconditionally verifiable blind computation, Phys. Rev. A **96**, 012303 (2017).

[16] T. Morimae and K. Fujii, Blind quantum computation protocol in which Alice only makes measurements, Phys. Rev. A **87**, 050301(R) (2013).

[17] V. Dunjko, E. Kashefi, and A. Leverrier, Blind Quantum Computing with Weak Coherent Pulses, Phys. Rev. Lett. **108**, 200502 (2012).

[18] M. Hajdušek, C. A. Perez-Delgado, and J. F. Fitzsimons, Device-independent verifiable blind quantum computation, arXiv:1502.02563.

[19] A. Gheorghiu, E. Kashefi, and P. Wallden, Robustness and device independence of verifiable blind quantum computing, New J. Phys. **17**, 083040 (2015).

[20] B. Reichardt, F. Unger, and U. Vazirani, Classical command of quantum systems, Nature (London) **496**, 456 (2013).

[21] M. McKague, Interactive proofs for BQP via self-tested graph states, Theory Comput. **12**, 1 (2016).

[22] T. Kapourniotis, E. Kashefi, and A. Datta, Verified delegated quantum computing with one pure qubit, arXiv:1403.1438.

[23] A. Broadbent, How to verify a quantum computation, Theory Comput. **14**, 1 (2018).

[24] M. Hayashi and T. Morimae, Verifiable Measurement-Only Blind Quantum Computing with Stabilizer Testing, Phys. Rev. Lett. **115**, 220502 (2015).

[25] T. Morimae, Measurement-only verifiable blind quantum computing with quantum input verification, Phys. Rev. A **94**, 042301 (2016).

[26] M. Hayashi and M. Hajdusek, Self-guaranteed measurement-based quantum computation, Phys. Rev. A **97**, 052308 (2018).

[27] A. Mantri, T. F. Demarie, N. C. Menicucci, and J. F. Fitzsimons, Flow Ambiguity: A Path Towards Classically Driven Blind Quantum Computation, Phys. Rev. X **7**, 031004 (2017).

[28] S. Barz, E. Kashefi, A. Broadbent, J. Fitzsimons, A. Zeilinger, and P. Walther, Demonstration of blind quantum computing, Science **335**, 303 (2012).

[29] S. Barz, J. Fitzsimons, E. Kashefi, and P. Walther, Experimental verification of quantum computation, Nat. Phys. **9**, 727 (2013).

[30] C. Greganti, M.-C. Roehsner, S. Barz, T. Morimae, and P. Walther, Demonstration of measurement-only blind quantum computing, New J. Phys. **18**, 013020 (2016).

[31] H.-L. Huang, Q. Zhao, X. Ma, C. Liu, Z.-E. Su, X.-L. Wang, L. Li, N.-L. Liu, B. C. Sanders *et al.*, Experimental Blind Quantum Computing for a Classical Client, Phys. Rev. Lett. **119**, 050503 (2017).

[32] T. Morimae, Continuous-Variable Blind Quantum Computation, Phys. Rev. Lett. **109**, 230502 (2012).

[33] K. Marshall, C. S. Jacobsen, C. Schäfermeier, T. Gehring, C. Weedbrook, and U. L. Andersen, Continuous-variable quantum computing on encrypted data, Nat. Commun. **7**, 13795 (2016).

[34] S. L. Braunstein and P. van Loock, Quantum information with continuous variables, Rev. Mod. Phys. **77**, 513 (2005).

[35] U. Andersen, G. Leuchs, and C. Silberhorn, Continuous-variable quantum information processing, Laser Photonics Rev. **4**, 337 (2010).

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

[37] K. Marshall, R. Pooser, G. Siopsis, and C. Weedbrook, Quantum simulation of quantum field theory using continuous variables, Phys. Rev. A **92**, 063825 (2015).

[38] N. Liu, J. Thompson, C. Weedbrook, S. Lloyd, V. Vedral, M. Gu, and K. Modi, Power of one qumode for quantum computation, Phys. Rev. A **93**, 052304 (2016).

[39] H.-K. Lau, R. Pooser, G. Siopsis, and C. Weedbrook, Quantum Machine Learning Over Infinite Dimensions, Phys. Rev. Lett. **118**, 080501 (2017).

[40] T. F. Demarie, T. Linjordet, N. C. Menicucci, and G. K. Brennen, Detecting topological entanglement entropy in a lattice of quantum harmonic oscillators, New J. Phys. **16**, 085011 (2014).

[41] F. Grosshans and P. Grangier, Continuous Variable Quantum Cryptography Using Coherent States, Phys. Rev. Lett. **88**, 057902 (2002).

[42] N. C. Menicucci, B. Q. Baragiola, T. F. Demarie, and G. K. Brennen, Anonymous broadcasting of classical information with a continuous-variable topological quantum code, Phys. Rev. A **97**, 032345 (2018).

[43] T. Douce, D. Markham, E. Kashefi, E. Diamanti, T. Coudreau, P. Milman, P. van Loock, and G. Ferrini, Continuous-Variable Instantaneous Quantum Computing is Hard to Sample, Phys. Rev. Lett. **118**, 070503 (2017).

[44] M. Yukawa, K. Miyata, H. Yonezawa, P. Marek, R. Filip, and A. Furusawa, Emulating quantum cubic nonlinearity, Phys. Rev. A **88**, 053816 (2013).

[45] K. Marshall, R. Pooser, G. Siopsis, and C. Weedbrook, Repeat-until-success cubic phase gate for universal continuous-variable quantum computation, Phys. Rev. A **91**, 032321 (2015).

[46] K. Miyata, H. Ogawa, P. Marek, R. Filip, H. Yonezawa, J.-i. Yoshikawa, and A. Furusawa, Implementation of a quantum cubic gate by an adaptive non-Gaussian measurement, Phys. Rev. A **93**, 022301 (2016).

[47] P. Marek, R. Filip, H. Ogawa, A. Sakaguchi, S. Takeda, J.-i. Yoshikawa, and A.Furusawa, General implementation of arbitrary nonlinear quadrature phase gates, Phys. Rev. A **97**, 022329 (2018).

[48] G. Adesso, S. Ragy, and A. R. Lee, Continuous variable quantum information: Gaussian states and beyond, Open Syst. Inf. Dyn. **21**, 1440001 (2014).

[49] S. D. Bartlett, B. C. Sanders, S. L. Braunstein, and K. Nemoto, Efficient Classical Simulation of Continuous Variable Quantum Information Processes, Phys. Rev. Lett. **88**, 097904 (2002).

[50] S. Lloyd and S. L. Braunstein, Quantum Computation Over Continuous Variables, Phys. Rev. Lett. **82**, 1784 (1999).

[51] D. Gottesman, A. Kitaev, and J. Preskill, Encoding a qubit in an oscillator, Phys. Rev. A **64**, 012310 (2001).

[52] L. Aolita, C. Gogolin, M. Kliesch, and J. Eisert, Reliable quantum certification of photonic state preparations, Nat. Commun. **6**, 8498 (2015).

[53] M. Gluza, M. Kliesch, J. Eisert, and L. Aolita, Fidelity Witnesses for Fermionic Quantum Simulations, Phys. Rev. Lett. **120**, 190501 (2018).

[54] S. Ghose and B. Sanders, Non-Gaussian ancilla states for continuous variable quantum computation via Gaussian maps, J. Mod. Opt. **54**, 855 (2007).

[55] M. Cramer, M. B. Plenio, S. T. Flammia, R. Somma, D. Gross, S. D. Bartlett, O. Landon-Cardinal, D. Poulin, and Y.-K. Liu, Efficient quantum state tomography, Nat. Commun. **1**, 149 (2010).

[56] D. Hangleiter, M. Kliesch, M. Schwarz, and J. Eisert, Direct certification of a class of quantum simulations, Quantum Sci. Technol. **2**, 015004 (2017).

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

[58] Y. Takeuchi and T. Morimae, Verification of Many-Qubit States, Phys. Rev. X **8**, 021060 (2018).

[59] S. T. Flammia and Y.-K. Liu, Direct Fidelity Estimation from Few Pauli Measurements, Phys. Rev. Lett. **106**, 230501 (2011).

[60] M. P. da Silva, O. Landon-Cardinal, and D. Poulin, Practical Characterization of Quantum Devices Without Tomography, Phys. Rev. Lett. **107**, 210404 (2011).

[61] R. J. Serfling, Probability inequalities for the sum in sampling without replacement, Ann. Stat. **2**, 39 (1974).

[62] Y. Takeuchi, A. Mantri, T. Morimae, A. Mizutani, and J. F. Fitzsimons, Resource-efficient verification of quantum computing using Serfling's bound, npj Quantum Inf. **5**, 27 (2019).

[63] N. C. Menicucci, P. van Loock, M. Gu, C. Weedbrook, T. C. Ralph, and M. A. Nielsen, Universal Quantum Computation with Continuous-Variable Cluster States, Phys. Rev. Lett. **97**, 110501 (2006).

[64] R. N. Alexander, S. Yokoyama, A. Furusawa, and N. C. Menicucci, Universal quantum computation with temporal-mode bilayer square lattices, Phys. Rev. A **97**, 032302 (2018).

[65] M. Ohliger and J. Eisert, Efficient measurement-based quantum computing with continuous-variable systems, Phys. Rev. A **85**, 062318 (2012).

[66] K. Vogel and H. Risken, Determination of quasiprobability distributions in terms of probability distributions for the rotated quadrature phase, Phys. Rev. A **40**, 2847 (1989).

[67] G. M. D'Ariano, L. Maccone, and M. F. Sacchi, Homodyne tomography and the reconstruction of quantum states of light, in *Quantum Information With Continuous Variables of Atoms and Light* (World Scientific, Singapore, 2007), pp. 141–158.

[68] A. Gheorghiu, T. Kapourniotis, and E. Kashefi, Verification of quantum computation: An overview of existing approaches, Theory Comput. Syst. **63**, 715 (2019).

[69] H.-A. Bachor and T. C. Ralph, *A Guide to Experiments in Quantum Optics* (Wiley, Weinheim, 2004).