Probabilistic fault-tolerant universal quantum computation and sampling problems in continuous variables

N.B. When citing this work, cite the original published paper.

(article starts on next page)

Probabilistic fault-tolerant universal quantum computation and sampling problems in continuous variables

Tom Douce,[1] Damian Markham,[2] Elham Kashefi,[1,2] Peter van Loock,[3] and Giulia Ferrini[3,4]

[1]*School of Informatics, University of Edinburgh, 10 Crichton Street, Edinburgh, EH8 9AB, United Kingdom*
[2]*Sorbonne Université, CNRS, Laboratoire d'Informatique de Paris 6, F-75005 Paris, France*
[3]*Institute of Physics, Johannes-Gutenberg Universität Mainz, Staudingerweg 7, 55128 Mainz, Germany*
[4]*Department of Microtechnology and Nanoscience (MC2), Chalmers University of Technology, SE-412 96 Gothenburg, Sweden*

Continuous-variable (CV) devices are a promising platform for demonstrating large-scale quantum information protocols. In this framework we define a general quantum computational model based on a CV hardware. It consists of vacuum input states, a finite set of gates—including non-Gaussian elements—and homodyne detection. We show that this model incorporates encodings sufficient for probabilistic fault-tolerant universal quantum computing. Furthermore, we show that this model can be adapted to yield sampling problems that cannot be simulated efficiently with a classical computer, unless the polynomial hierarchy collapses. This allows us to provide a simple paradigm for experiments to probe quantum advantage relying on Gaussian states, homodyne detection, and some form of non-Gaussian evolution. We finally address the recently introduced model of instantaneous quantum computing in CV, and prove that the hardness statement is robust with respect to some experimentally relevant simplifications in the definition of that model.

I. INTRODUCTION

Continuous-variable (CV) systems are emerging as promising candidates for the implementation of quantum computation (QC) models. The main reason for this interest relies in the possibility of generating deterministically large resource states such as cluster states, composed of up to one million modes [1]. More generally, the optical CV approach includes highly efficient ways to prepare and measure sophisticated quantum states. Furthermore, new experimental techniques that are not anymore purely optical are being addressed for CV quantum information, based, e.g., on microwaves resonators coupled to superconducting Josephson junctions [2,3], or on optomechanical resonators [4,5].

In contrast to their typically high efficiencies, optical CV schemes suffer from an intrinsic sensitivity to Gaussian errors such as photon loss and thermal noise. Standard approaches to quantum error correction, encoding a logical mode into many physical modes, have been proven to be inefficient when both the error itself and the operations for error correction are of Gaussian nature [6,7]. Nonetheless, codes have been proposed that can protect logical qubits encoded into one or more optical modes against errors induced, for instance, from photon loss [8–16]. In particular, those schemes encoding discrete logical information into a single optical mode, such as the so-called cat codes [13–16], are sometimes referred to as CV codes. The very first proposal of such a CV code is the famous Gottesmann-Kitaev-Preskill (GKP) encoding that later has been shown to allow for universal fault-tolerant quantum computation in the measurement-based scenario [17,18]. This encoding uses highly non-Gaussian states, the so-called GKP states, in order to encode DV quantum information on a CV hardware, namely onto the infinite dimensional Hilbert space of a single harmonic oscillator. These states possess a comblike wave function, with peaks equally spaced placed at even (odd) multiples of $\sqrt{\pi}$ for the 0-logical state (1-logical state). GKP states have also been used as ancillary input states in a recently defined sampling model in CV, namely instantaneous quantum polytime (IQP) [19], whose output probability distribution was shown to be hard to sample. However, these states are rather hard to produce, and only recently their experimental generation has been tackled [20]. This practical difficulty makes it desirable to define both a model of fault-tolerant CV quantum computation and sampling models that are hard to classically simulate, which do not explicitly require GKP states as ancillary states at the input of the model.

In this work we address these two aspects. On the one hand, we define a model for universal fault-tolerant quantum computation in CV where GKP states are probabilistically generated within the model itself. Similar to the original version of an in-principle efficient, universal and to some extent fault-tolerant linear-optics quantum computer based on probabilistic quantum gates with single-photon states, the well-known KLM model [21], our model as presented here is also intended as an especially conceptual step forward rather than an immediately implementable proposal. Indeed, its typical success probabilities may be too low to yield an experimentally practical and scalable solution for universal quantum computation with today's technology. However, it allows us to show that, in principle, a number of ancillary modes set in the vacuum state, a polynomial number of gates drawn from an elementary gate set, and homodyne detection, are sufficient for probabilistic universal fault-tolerant quantum computation. Compared to Ref. [22], we show that a finite set of gates, characterized by specific values of the gate

parameters rather than a continuum, is sufficient for quantum computing with vacuum states.

On the other hand, we later specialize to sampling models and show that models that are hard to classically sample up to relative error can be defined, where no GKP state is needed at the input, thereby improving the results of Ref. [19] and obtaining more experimentally friendly architectures. These models are solely based on homodyne detection for the required measurements.

As a common ground for both applications, we provide an explicit protocol for the probabilistic generation of GKP states, by starting from vacua, a given set of elementary quantum gates and using homodyne detection. This generation method is based on the protocol of Ref. [23] that uses input squeezed cat states, beam splitters, and homodyne measurements. We further provide an explicit decomposition of the cross-Kerr interaction utilized to generate the cat states in terms of elementary gates that belong to our models. In this way, GKP generation is subsumed within the models themselves. As an important point, the definition of the gates in our models depends on the tolerated error probability on the computation result.

The paper is structured as follows. In Sec. II we recall the basics of GKP encoding. In Sec. III we set the problem and define in more detail the models we are interested in. Section IV is dedicated to the description and characterization of the specific protocol used to generate GKP states. Then Secs. V and VI discuss the issue of fault tolerance and its implications in the universal as well as in the subuniversal sampling models. Finally, conclusions and perspectives are presented in Sec. VII. Throughout the paper we adopt the convention $[\hat{q}, \hat{p}] = i$ for the quadratures commutator, which corresponds to the relation $\hat{a} = (\hat{q} + i\hat{p})/\sqrt{2}$ and fixes the vacuum fluctuations to $\Delta^2 q_0 \equiv \Delta^2 p_0 = 1/2$.

II. RECALLING THE GKP ENCODING

GKP states are highly non-Gaussian states with a comb-like wave function. They allow us to encode a qubit into a harmonic oscillator's Hilbert space. Ideal GKP states, which we denote as $|0_L\rangle$, $|1_L\rangle$, are defined as wave functions made of an infinite number of Dirac peaks [17]:

$$
\begin{aligned}
|0_L\rangle &= \sum_n |2n\sqrt{\pi}\rangle_q = \sum_n |n\sqrt{\pi}\rangle_p, \\
|1_L\rangle &= \sum_n |(2n+1)\sqrt{\pi}\rangle_q = \sum_n (-1)^n |n\sqrt{\pi}\rangle_p,
\end{aligned} \tag{1}
$$

where $|s\rangle_q$ ($|t\rangle_p$) denotes the eigenstate of the position operator of eigenvalue s (momentum operator of eigenvalue t). In the following we will omit the subscript when the situation is unambiguous. These states realize a one-to-one correspondence between Clifford qubit operations and Gaussian transformations. More formally, the Clifford group is mapped to Gaussian transformations as follows:

$$
e^{i\sqrt{\pi}\hat{q}} \to \hat{Z}, \quad e^{i\hat{q}_1\hat{q}_2} \to \hat{C}_Z, \quad \hat{F} = e^{i\frac{\pi}{4}(\hat{p}^2 + \hat{q}^2)} \to \hat{H}, \tag{2}
$$

while the non-Clifford $\hat{T}$ gate is mapped as

$$
e^{i\frac{\pi}{4}\left[2\left(\frac{\hat{q}}{\sqrt{\pi}}\right)^3 + \left(\frac{\hat{q}}{\sqrt{\pi}}\right)^2 - 2\frac{\hat{q}}{\sqrt{\pi}}\right]} \to \hat{T}. \tag{3}
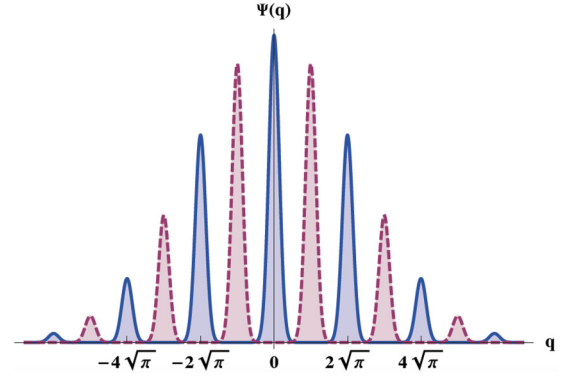$$

FIG. 1. Wave function in position representation of the GKP $|0_G\rangle$ state in continuous blue ($|1_G\rangle$ in dashed red) with $\delta = \sigma = 0.25$ from Eq. (4).

Realistic logical qubit states, which we indicate with $|0_G\rangle$, $|1_G\rangle$, are instead normalizable states, accounting for finite squeezing. Each Dirac peak is replaced by a normalized Gaussian of width σ, while the infinite sum itself becomes a Gaussian envelope function of width δ^{-1} (see Fig. 1). Because of this and despite the fact that they are highly non-Gaussian states, we will refer to these states as to Gaussian GKP states in the following. The resulting wave functions are

$$
\begin{aligned}
\langle q|0_G\rangle &= \int du\, dv\, G(u)F(v)\langle q|e^{-iu\hat{p}} e^{-iv\hat{q}}|0\rangle_L \\
&= N_0 \sum_n \exp\left(-\frac{(2n)^2 \pi \delta^2}{2}\right) \exp\left(-\frac{(q - 2n\sqrt{\pi})^2}{2\sigma^2}\right),
\end{aligned} \tag{4}
$$

$$
\begin{aligned}
\langle q|1_G\rangle &= \int du\, dv\, G(u)F(v)\langle q|e^{-iu\hat{p}} e^{-iv\hat{q}}|1\rangle_L \\
&= N_1 \sum_n \exp\left(-\frac{(2n+1)^2 \pi \delta^2}{2}\right) \\
&\quad \times \exp\left(-\frac{[q - (2n+1)\sqrt{\pi}]^2}{2\sigma^2}\right),
\end{aligned} \tag{5}
$$

where we have introduced the Gaussian noise distributions

$$
G(u) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{u^2}{2\sigma^2}}, \quad F(v) = \frac{1}{\delta\sqrt{2\pi}} e^{-\frac{v^2}{2\delta^2}}, \tag{6}
$$

and N_0 and N_1 are normalization constants. In the following, for conceptual clarity as well as simplicity, we consider symmetric GKP states, which have symmetric noise properties in the two quadratures, and are characterized by $\sigma = \delta$.

Ancillary $|0_G\rangle$ GKP states serve as resources to achieve fault tolerance in CV [17,18]. The idea in [17] is to entangle the state to be corrected at a given step of the computation with an ancillary GKP state, and then measure the ancillary modes by means of homodyne detection. One can show that in this way the noise in the $\hat{q}$ quadrature of a GKP encoded quantum state can be replaced by the noise of the ancillary $|0_G\rangle$ state. Repeating this gadget after a Fourier transform allows for correction of the other quadrature, thereby keeping the error below a desired amount. In Sec. V we address in

detail how this error-correction procedure can be used in order to ensure fault tolerance in our model.

III. DEFINITION OF THE MODELS

In this section we define the quantum computational models we are interested in. We first describe the CV universal quantum computational model. Then we turn to subuniversal models and define the corresponding sampling problems.

A. Probabilistic universal fault-tolerant quantum computation in CV

Our model for probabilistic, universal and fault-tolerant quantum computing in CV is based upon the following elements:

(i) The multimode input state is initialized in the vacuum $|0\rangle^{\otimes m}$, where m is the total number of modes.

(ii) The gates composing the circuit are drawn from the following finite sets:

$$A_1 = \left\{ e^{id\hat{q}}, e^{is\hat{q}^2}, e^{ic\hat{q}^3}, e^{ib\hat{q}_1\hat{q}_2} \right\}, \qquad (7)$$

$$A_2 = \left\{ e^{i\hat{q}\sqrt{\pi}}, e^{i\frac{\pi}{4}(\hat{p}^2+\hat{q}^2)}, e^{i\hat{q}_1\hat{q}_2}, e^{i\frac{\pi}{4}\left[2\left(\frac{\hat{q}}{\sqrt{\pi}}\right)^3+\left(\frac{\hat{q}}{\sqrt{\pi}}\right)^2-2\frac{\hat{q}}{\sqrt{\pi}}\right]} \right\}, \quad (8)$$

where the parameters in A_1 will be fixed later. They will be determined by the desired precision on the computation result. In contrast to Ref. [22], the CV gates in Eqs. (7) and (8) are characterized by specific values of the gate parameters, instead of spanning the full real axis. The linear and quadratic gates in Eqs. (7) and (8) are generally regarded as experimentally feasible. Note that $e^{i\frac{\pi}{4}(\hat{p}^2+\hat{q}^2)} \equiv \hat{F}$ is simply the Fourier transform. A non-Gaussian, experimentally challenging gate has also been included in A_1 (with powers greater than 2 in $\hat{q}$ and/or $\hat{p}$), and a similar non-Gaussian gate appears in A_2.

(iii) The measurements are done via homodyne detection in the momentum quadrature, i.e., by measuring $\hat{p}$, which corresponds to approximately measuring in the GKP basis $\{|+/-_G\rangle\}$ [17]. The homodyne detection may have a finite resolution, which is modeled by the finitely resolved $\hat{p}^\eta$ operator defined as [19,24]

$$\hat{p}^\eta = \sum_{k=-\infty}^{\infty} p_k \int_{-\infty}^{\infty} dp\, \chi_k^\eta(p)|p\rangle\langle p| \equiv \sum_{k=-\infty}^{\infty} p_k \hat{P}_k, \quad (9)$$

with $\chi_k^\eta(p) = 1$ for $p \in [p_k - \eta, p_k + \eta]$ and 0 outside, $p_k = 2\eta k$ and 2η the resolution, associated with the width of the detector pixels. As a technical remark, note that, provided that we can find an integer K such that $\sqrt{\pi} = K\eta$, this binning is consistent with the dichotomy at the level of logical measurements.

We prove that this model is at least as powerful as the standard qubit-based quantum computers by showing that any bounded quantum polynomial (BQP) [25] instance decided by a quantum circuit working with qubits can be mapped to a probabilistic CV circuit with a constant overhead. As mentioned above, the mapping relies on the ability to encode qubits in a quantum harmonic oscillator through the GKP procedure. More specifically we first have to generate (probabilistically) the GKP qubits in CV by applying the gate
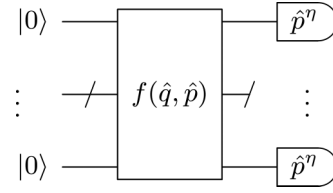

FIG. 2. Sampling architecture with Gaussian input state and homodyne detection. The finitely resolved homodyne measurement $\hat{p}^\eta$ has resolution 2η.

set A_1 and the Fourier transform upon several vacuum states. Then we use the gate set A_2: it is the exact analog of the universal DV gate set in the subspace spanned by the GKP states $\{|0/1_G\rangle\}$—as presented in Eqs. (2) and (3). Finally, the noise issue can be addressed using a combination of gates following the discussion in Sec. V.

B. Subuniversal models and sampling

Beyond fault-tolerant universal quantum computation, we address two subuniversal models of quantum computation that are associated with two respective sampling problems.

1. CV random circuit sampling

The first subuniversal model that we consider is illustrated in Fig. 2. This family of circuits share the same elementary gates as the universal model defined in Sec. III A, namely the gate sets A_1 in Eq. (7) and A_2 in Eq. (8).

In analogy to the family of circuits with random gates drawn from an elementary set for qubits, we refer to this architecture as to CV random circuit sampling [26]. Finite resolution in the homodyne detection ensures that we can associate well-defined probabilities to the continuous measurement outcomes through binning. Note that the detection modeled in Eq. (9) is equivalent to perfectly resolved homodyne detectors followed by a discretization (binning) of the measurement outcomes.

This model is not universal anymore, since the randomness occurring at the level of the measurement is not counteracted by post-selection. Nevertheless, we show that exact sampling—or equivalently sampling up to relative error—from the probability distribution of the measurement outcomes of the circuit family shown in Fig. 2 is classically hard, in the worst case scenario.

2. CV Instantaneous quantum computing with input squeezed states

The second subuniversal model we are interested in is IQP in CV, also said CVIQP [19] (Fig. 3).

This model is composed of the same elementary gates as those of the model in Fig. 2, except for the Fourier transform, namely

$$\tilde{A}_1 = \left\{ e^{i\tilde{d}\hat{q}}, e^{i\tilde{s}\hat{q}^2}, e^{i\tilde{c}\hat{q}^3}, e^{i\tilde{b}\hat{q}_1\hat{q}_2} \right\}, \qquad (10)$$

$$\tilde{A}_2 = \left\{ e^{i\hat{q}\sqrt{\pi}}, e^{i\hat{q}_1\hat{q}_2}, e^{i\frac{\pi}{4}\left[2\left(\frac{\hat{q}}{\sqrt{\pi}}\right)^3+\left(\frac{\hat{q}}{\sqrt{\pi}}\right)^2-2\frac{\hat{q}}{\sqrt{\pi}}\right]} \right\}. \qquad (11)$$

Therefore, all the gates in this model are diagonal in the position representation. We require momentum squeezed states
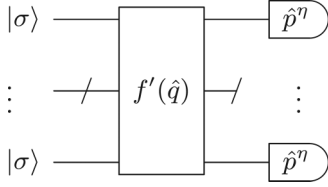
FIG. 3. IQP circuit in CVs. $|\sigma\rangle$ are finitely squeezed states with variance σ in the $\hat{p}$ representation. The gate $f'(\hat{q})$ is a uniform combination of elementary gates from the set in Eqs. (10) and (11). The finitely resolved homodyne measurement $\hat{p}^\eta$ has resolution 2η.

$|\sigma\rangle$ with $\sigma < 1$ to be present at the input. This model is a simpler version than that introduced in Ref. [19]. Specifically we show here that (i) we do not need GKP states as resource states and (ii) the squeezing parameter in the input states is constant and does not depend on the circuit size. These features make the present model more experimentally realistic, and yet we will prove that it retains its classical hardness (again for the exact probability distribution, and in the worst-case scenario).

The proofs of computational hardness for both sampling models, as well as the universality of the computational model presented in Sec. III A, will be based on the ability to synthesize GKP states by means of a sequence of the elementary gates that belong to the models themselves. To this end, in the following section we show how the approximate GKP states generation can be decomposed in terms of elementary gates.

IV. APPROXIMATE GKP STATES FROM A FINITE SET OF CV GATES

The main result we prove in this section is that there exists a finite number of CV gates that combined together allow one to generate approximate GKP states using vacuum input states and homodyne detection.

Our protocol for GKP generation can be divided into two steps: (1) probabilistic generation of cat states from vacua; and (2) probabilistic generation of approximate GKP states from cat states. The former protocol is based on that of Ref. [27] and on gate decomposition [28], while the latter is based on Ref. [23]. We detail here below first step 2 and later step 1, focusing on the respective associated fidelities and success probabilities. The following subsections are rather technical and the uninterested reader may skip them and move to Sec. V where we take advantage of this protocol.

A. GKP states from cat states

The protocol designed by Vasconcelos and co-authors in [23] relies on squeezed cat states combined in a linear optical network and measured by homodyne detection. The basic idea is (i) prepare two cat states $|\alpha\rangle + |-\alpha\rangle$ of real amplitude α, (ii) squeeze them to reproduce the squeezing of the peaks in a GKP state, (iii) send them to a balanced BS, and (iv) measure the $\hat{p}$ quadrature of one the modes. If the outcome of the homodyne detection is 0, the output state contains three Gaussian peaks enveloped by a binomial distribution, i.e., it is a *binomial state*, that approximates a GKP state. For this reason, and in order to avoid confusion with the binomial codes introduced in Ref. [12], we will refer to these states
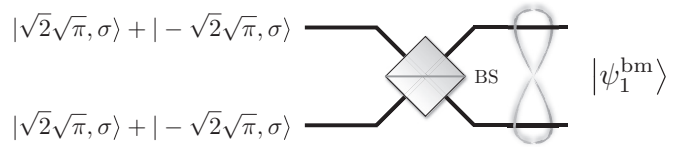

FIG. 4. First iteration of the protocol of Ref. [23] for the probabilistic generation of binomial GKP states: two cat states are squeezed, then combined, at a beam splitter. The $\hat{p}$ quadrature is then measured in one of the output modes.

as to binomial GKP states in what follows. The first iteration of this scheme is illustrated in Fig. 4. This scheme can then be repeated to produce higher order binomial GKP states possessing a larger number of peaks, better approximating Gaussian GKP states. More specifically, the mth binomial GKP state's position wave function reads

$$_q\langle q|0_m\rangle = \frac{\pi^{-1/4}}{\sqrt{\binom{2^{m+1}}{2^m}}\sigma} \sum_{i=0}^{2^m} \binom{2^m}{i} e^{-\frac{[q-2\sqrt{\pi}(i-2^{m-1})]^2}{2\sigma^2}}, \qquad (12)$$

where σ characterizes the squeezing of each peak. In general, let m be a positive integer. We set the amplitude of the cat states to $\alpha_m = \sqrt{2}^{m-1}\sqrt{\pi}\sigma^{-1}$, where σ corresponds to the amount of squeezing of the individual peaks in the GKP position wave function.

1. Quantification of the quality of the binomial GKP states

We compare the binomial GKP states obtained through this procedure to the standard Gaussian GKP states in Eq. (1). We stress that in a binomial GKP state, although the individual peaks are standard Gaussians, the envelope is described by binomial coefficients. More specifically, the weight of the ith peak, in terms of probabilities, is given by

$$\frac{1}{\binom{2^{m+1}}{2^m}}\binom{2^m}{i}^2 \qquad (13)$$

instead of the Gaussian function characterized by a squeezing parameter given in Eq. (4). We aim at finding the closest Gaussian function approximating the distribution in Eq. (13). Using the central limit theorem in the limit of large m, the binomial distribution of parameters 2^m and $1/2$ leads to a normal distribution of mean 2^{m-1} and variance 2^{m-2}. Mathematically it means we have the following relation:

$$\frac{1}{2^{2^m}}\binom{2^m}{i} \approx \frac{1}{\sqrt{2\pi 2^{m-2}}} \exp\left(-\frac{(2^{m-1}-i)^2}{2 \times 2^{m-2}}\right). \qquad (14)$$

So necessarily the distribution in Eq. (13), which corresponds to the left-hand-side squared, will be associated with a Gaussian of mean 2^{m-1} and variance 2^{m-3}. Taking into account the proper normalization we obtain

$$\frac{1}{\binom{2^{m+1}}{2^m}}\binom{2^m}{i}^2 \approx \frac{1}{\sqrt{2\pi 2^{m-3}}} \exp\left(-\frac{(2^{m-1}-i)^2}{2 \times 2^{m-3}}\right). \qquad (15)$$

TABLE I. Comparison between binomial GKP states and their closest Gaussian GKP counterpart and success probability of the protocol to generate them, according to Eq. (29). The overlap is determined using Eq. (16). Recall that the number of peaks scales as $2^m + 1$ and that the results derived here assume $\eta\sigma < 1$.

m	Squeezing equivalent	Overlap with Gaussian GKP	Success probability
1	5 dB	0.9976	$1.7\eta\sigma$
2	8 dB	0.9986	$6.3(\eta\sigma)^3$
3	11 dB	0.9997	$1.2 \times 10^2 (\eta\sigma)^7$
4	14 dB	0.9999	$5.6 \times 10^4 (\eta\sigma)^{15}$

In a standard, Gaussian enveloped GKP state, recall from Eq. (4) that the weight reads $\exp[-(2j\sqrt{\pi})^2\sigma^2/2]$ for the jth peak of the wave function. Using Eq. (14) it yields for the corresponding squeezing parameter σ:

$$\sigma^2 = \frac{1}{2^m\pi}. \tag{16}$$

We stress that due to Eq. (16) the effective squeezing in the binomial GKP states depends on the number of iterations of the protocol: the higher the number of iterations, the higher the squeezing. Thus we have identified the closest Gaussian GKP state to the binomial GKP state of Eq. (13). Its position wave function reads

$$_q\langle q|0_G\rangle = \frac{(2^{m-2})^{-1/4}}{\sqrt{\sigma\pi}} \sum_{j=-\infty}^{+\infty} e^{-\frac{(2j\sqrt{\pi})^2}{2\times 2^m\pi}} e^{-\frac{(q-2j\sqrt{\pi})^2}{2\sigma^2}}. \tag{17}$$

We may now compute the fidelity between the binomial GKP state produced through the protocol of Ref. [23] and the Gaussian GKP state. To simplify the calculations we assume that the Gaussian peaks are narrow enough to be considered as orthogonal. The inner product thus reads

$$|\langle 0_m|0_G\rangle| \approx \frac{\pi^{-1/4}(2^{m-2})^{-1/4}}{\sqrt{\binom{2^{m+1}}{2^m}}} \sum_{i=0}^{2^m} \sum_{j=-\infty}^{+\infty} \binom{2^m}{i} e^{-\frac{(2j\sqrt{\pi})^2}{2\times 2^m\pi}}$$
$$\times \int dq \frac{1}{\sqrt{\pi}\sigma} e^{-\frac{[q-2\sqrt{\pi}(i-2^{m-1})]^2}{2\sigma^2}} e^{-\frac{(q-2j\sqrt{\pi})^2}{2\sigma^2}}. \tag{18}$$

This assumption also implies that the integral vanishes except for the $2^m + 1$ cases when $j = i - 2^{m-1}$, and it is then properly normalized. So we simply have to focus on the overlap of the envelopes, namely

$$|\langle 0_m|0_G\rangle| \approx \frac{\pi^{-1/4}(2^{m-2})^{-1/4}}{\sqrt{\binom{2^{m+1}}{2^m}}} \sum_{i=0}^{2^m} \binom{2^m}{i} e^{-\frac{(i-2^{m-1})^2}{2^{m-1}}}. \tag{19}$$

Table I summarizes the results for different values of the iteration parameter m. Note that the fidelity between binomial and Gaussian GKP states becomes quite large already for few iterations.

2. Finite resolution and success probability

The protocol for GKP states synthesis from cat states that we have described above is probabilistic, and indeed it works only if all $2^m - 1$ homodyne detections yield outcome 0. In order for the success probability not to vanish completely,

homodyne detection must have finite resolution. Hence we introduce a resolution η for the homodyne detection as a binning of the real axis, consistently with Eq. (9). The projector on outcome zero associated with all homodyne detections thus reads

$$P_0^m = \int_{-\eta}^{\eta} d\mathbf{s}|\mathbf{s}\rangle_\mathbf{p}\langle\mathbf{s}|, \tag{20}$$

where $\mathbf{s}$ is a $2^m - 1$ dimensional real vector and the integration is over the box $[-\eta, \eta]^{2^m-1}$. In the following we quantify the success probability associated with GKP state synthesis using this detection binning.

We first focus on the 2^m-mode quantum state $|\psi_m^{\text{bm}}\rangle$ right before the measurements are performed. We denote $|\alpha, \sigma\rangle$ a displaced squeezed vacuum state, where $\alpha \in \mathbb{R}$ corresponds to the displacement and σ to its squeezing. The position wave function of such a state is

$$_q\langle q|\alpha, \sigma\rangle = \frac{1}{\pi^{1/4}\sigma^{1/2}} \int dq\, e^{-\frac{(q-\sqrt{2}\alpha)^2}{2\sigma^2}}. \tag{21}$$

We consider as input state the squeezed cat state. With these notations, the input state $|\psi_m^{\text{in}}\rangle$ to generate the mth binomial GKP state is merely

$$|\psi_m^{\text{in}}\rangle = \frac{1}{\sqrt{N}} \bigotimes_{i=1}^{2^m} (|\alpha_m, \sigma\rangle_i + |-\alpha_m, \sigma\rangle_i), \tag{22}$$

where the subscript i labels the mode, $\alpha_m = \sqrt{2}^m\sqrt{\pi}$, and N is the state norm. Note that, in this simple case, the action of a beam splitter on two identically squeezed states reads

$$|\mu, \sigma\rangle|\lambda, \sigma\rangle \xmapsto{\text{BS}} \left|\frac{\mu-\lambda}{\sqrt{2}}, \sigma\right\rangle\left|\frac{\mu+\lambda}{\sqrt{2}}, \sigma\right\rangle. \tag{23}$$

So the global state after the beam splitters is a sum of many 2^m-fold tensorial products involving displaced squeezed states. We can actually isolate the output mode and using combinatorial arguments finally write down $|\psi_m^{\text{bm}}\rangle$:

$$|\psi_m^{\text{bm}}\rangle = \frac{1}{\sqrt{N}} \sum_{i=-2^{m-1}}^{2^{m-1}} |2i\sqrt{\pi}, \sigma\rangle$$
$$\times \sum_{j=1}^{\binom{2^m}{2^{m-1}+i}} |\alpha_1^{i,j}, \sigma\rangle \cdots |\alpha_{2^m-1}^{i,j}, \sigma\rangle, \tag{24}$$

where the $\alpha_k^{i,j}$'s are multiples of $\sqrt{\pi}$ and bounded in absolute value by $2^{m-1}\sqrt{\pi}$.

Now recall that the momentum wave function of a displaced squeezed vacuum state of real amplitude α reads

$$_p\langle s|\alpha, \sigma\rangle = \frac{\sqrt{\sigma}}{\pi^{1/4}} e^{-i\sqrt{2}\alpha s} e^{-\frac{s^2\sigma^2}{2}}. \tag{25}$$

Let ρ_r be the density matrix obtained after tracing out the unmeasured mode. Starting from Eq. (24), we have (note the relabeling of the variables)

$$\rho_r = \frac{1}{N} \sum_{i=0}^{2^m} \sum_{j,j'=1}^{\binom{2^m}{i}} |\alpha_1^{i,j}, \sigma\rangle \cdots |\alpha_{2^m-1}^{i,j}, \sigma\rangle\langle\alpha_1^{i,j'}, \sigma| \cdots \langle\alpha_{2^m-1}^{i,j'}, \sigma|.$$

$$\tag{26}$$

We may now derive the success probability of the protocol, i.e., the probability that $2^m - 1$ homodyne detections yield outcome 0. In the state before the measurement, the maximum (absolute) value of all amplitudes is $2^{m-1}\sqrt{\pi}$. So if $\eta 2^{m-1}\sqrt{\pi} \ll 1$ and $\eta\sigma_m \ll 1$ [and only the first assumption is sufficient if Eq. (16) holds] we have from Eq. (25):

$$_p\langle s|\alpha_k^{l,l'}, \sigma_m\rangle \approx \frac{\sqrt{\sigma_m}}{\pi^{1/4}}, \tag{27}$$

for all triples (k, l, l') and all $s \in [-\eta, \eta]$. The probability of hitting 0 for all measurements, $p_m(0)$, is then given by

$$p_m(0) = \text{Tr}[P_m(0)\rho_r] = \int_{-\eta}^{\eta} d\mathbf{s}\langle\mathbf{s}|\rho_\mathbf{r}|\mathbf{s}\rangle. \tag{28}$$

Using Eq. (27) we get

$$
\begin{aligned}
p_m(0) &= \frac{1}{N}\int_{-\eta}^{\eta} d\mathbf{s} \sum_{i=0}^{2^m}\sum_{j,j'=1}^{\binom{2^m}{i}} \left|\left(\frac{\sqrt{\sigma_m}}{\pi^{1/4}}\right)^{2^m-1}\right|^2 \\
&= \frac{1}{N}\int_{-\eta}^{\eta} d\mathbf{s}\left(\frac{\sigma_m}{\sqrt{\pi}}\right)^{2^m-1}\sum_{i=0}^{2^m}\binom{2^m}{i}^2 \\
&= \frac{1}{N}(2\eta)^{2^m-1}\left(\frac{\sigma_m}{\sqrt{\pi}}\right)^{2^m-1}\binom{2^{m+1}}{2^m} \\
&= \frac{1}{2^{2^m}}\binom{2^{m+1}}{2^m}\left(\frac{2\eta\sigma_m}{\sqrt{\pi}}\right)^{2^m-1}. \tag{29}
\end{aligned}
$$

In Table I we show the expected success probabilities for different values of m. To give an idea we study the limit of large m where we have $\binom{2^{m+1}}{2^m} \sim 4^{2^m}/(\sqrt{\pi}\sqrt{2^m})$. It means that the success probability behaves asymptotically as

$$p_m(0) \sim \frac{1}{2\sqrt{2^m}}\left(\frac{4}{\sqrt{\pi}}\right)^{2^m}(\eta\sigma_m)^{2^m-1}. \tag{30}$$

Recall that this expression is valid under the constraint that $\eta\sigma_m \ll 1$. So in particular $\eta\sigma_m 4/\sqrt{\pi} < 1$, which ensures that the probability remains well defined. Also note that the notion of scaling is absent from these considerations. Both η and σ_m are fixed parameters here.

3. Impact on the output state

We now focus on the quality of the actual output binomial GKP state after measuring the $2^m - 1$ ancillary modes. We still consider that the resolution obeys the two conditions mentioned above, namely $\eta 2^{m-1} \ll 1$ and $\eta\sigma_m \ll 1$. We can show that in this case the state is actually exactly the correct pure binomial GKP state. We are going to derive this explicitly for the two-mode scenario depicted in Fig. 4, which corresponds to the binomial GKP state made of three peaks.

We use the mapping in Eq. (23) for two identical squeezed cat states at the input $|\sqrt{2}\sqrt{\pi}, \sigma\rangle + |-\sqrt{2}\sqrt{\pi}, \sigma\rangle$, where $\sigma < 1$. We obtain a two-mode entangled state that reads—with the convention that the first and second ket denotes the upper and lower mode:

$$
\begin{aligned}
|\psi_1^{\text{bm}}\rangle &= \frac{1}{\sqrt{N}}[|0\rangle|-2\sqrt{\pi}, \sigma\rangle + (|2\sqrt{\pi}, \sigma\rangle \\
&\quad + |-2\sqrt{\pi}, \sigma\rangle)|0\rangle + |0\rangle|2\sqrt{\pi}, \sigma\rangle], \tag{31}
\end{aligned}
$$

where N is the normalization constant. The upper mode is measured in the $\hat{p}$ quadrature and the outcome 0 is recorded. If we suppose that the resolution satisfies $\eta 2\sqrt{\pi} = o(1)$ and $\eta\sigma = o(1)$, then Eq. (27) still holds. With the notations of this section we have for all $s \in [-\eta, \eta]$ and all $\beta = 0, \pm 2\sqrt{\pi}$:

$$_p\langle s|\beta, \sigma\rangle \approx \frac{\sqrt{\sigma}}{\pi^{1/4}}. \tag{32}$$

Recall that we assume that the displaced squeezed vacuum states are orthogonal to each other. Then the reduced density matrix for the mode being measured ρ_r after tracing over the unmeasured mode reads

$$
\begin{aligned}
\rho_r &= \text{Tr}_{\text{low}}\big[|\psi_1^{\text{bm}}\rangle\langle\psi_1^{\text{bm}}|\big] \\
&= \frac{1}{4}[2|0, \sigma\rangle\langle 0, \sigma| + (|2\sqrt{\pi}, \sigma\rangle + |-2\sqrt{\pi}, \sigma\rangle) \\
&\quad \times (\langle 2\sqrt{\pi}, \sigma| + \langle -2\sqrt{\pi}, \sigma|)], \tag{33}
\end{aligned}
$$

so that the success probability yields, under the assumptions leading to Eq. (32):

$$
\begin{aligned}
p_1(0) &= \int_{-\eta}^{\eta} ds\langle s|\rho_r|s\rangle \\
&= \frac{1}{4}\int_{-\eta}^{\eta} ds[2|_p\langle s|0, \sigma\rangle|^2 + |_p\langle s|(|2\sqrt{\pi}, \sigma\rangle \\
&\quad + |-2\sqrt{\pi}, \sigma\rangle)|^2] \\
&= \frac{1}{4}\left[2\times 2\eta\frac{\sigma}{\sqrt{\pi}} + 4\times 2\eta\frac{\sigma}{\sqrt{\pi}}\right] \\
&= \frac{3\eta\sigma}{\sqrt{\pi}}. \tag{34}
\end{aligned}
$$

We can easily check that this is consistent with the general formula derived in Eq. (29). We may now compute the output state after obtaining outcome 0 at the measurement. It reads

$$\rho_1 = \frac{\text{Tr}_{\text{up}}\big[P_1(0)|\psi_1^{\text{bm}}\rangle\langle\psi_1^{\text{bm}}|\big]}{p_1(0)}, \tag{35}$$

where $P_1(0) = \int_{-\eta}^{\eta} ds|s\rangle_p\langle s|$ is the projector associated with outcome 0 and the upper mode. Then we have

$$
\begin{aligned}
\rho_1 &= \frac{1}{p_1(0)}\left(\int_{-\eta}^{\eta} ds_p\langle s|\psi_1^{\text{bm}}\rangle\langle\psi_1^{\text{bm}}|s\rangle_p\right) \\
&= \frac{1}{6}(|2\sqrt{\pi}, \sigma\rangle + 2|0, \sigma\rangle + |-2\sqrt{\pi}, \sigma\rangle) \\
&\quad \times (\langle 2\sqrt{\pi}, \sigma| + 2\langle 0, \sigma| + \langle -2\sqrt{\pi}, \sigma|), \tag{36}
\end{aligned}
$$

which is indeed a pure state corresponding to the definition of the first binomial GKP state. This reasoning can be extended

by induction to show that binomial GKP states are pure at all orders for a good enough resolution.

Now that we have studied and characterized the binomial GKP states that can be generated using Schrödinger cat states we will describe a protocol that approximately generates the latter using vacuum states.

B. Cat states from coherent states

The protocol for binomial GKP state generation that we have outlined above is based on the use of cat states of the form

$$\frac{1}{\sqrt{N}}(|\alpha\rangle + |-\alpha\rangle). \tag{37}$$

In the following we assume that all coherent states amplitudes are large enough so that the coherent states in Eq. (37) can be considered as orthogonal. In particular it means that $N = 2$ in Eq. (37).

In this section we detail how these states can be generated probabilistically and approximately given a set of elementary gates and homodyne detection. We use the probabilistic protocol of Ref. [27]. A π-strength cross-Kerr interaction acting on two coherent states of amplitudes $|\alpha_0\rangle$ and $|\beta_0\rangle$ yields

$$e^{i\pi\hat{n}_1\hat{n}_2}|\alpha_0\rangle|\beta_0\rangle = \frac{1}{2}(|\alpha_0\rangle + |-\alpha_0\rangle)|\beta_0\rangle \\ + \frac{1}{2}(|\alpha_0\rangle - |-\alpha_0\rangle)|-\beta_0\rangle. \tag{38}$$

We see from Eq. (38) that if by measuring the second mode one can infer an amplitude of β_0, then the first mode is projected onto the cat state we are interested in given by Eq. (37), with coherent components of amplitude α_0. Since the probability density for homodyne detection on the second mode consists of two Gaussians at $\pm\beta_0$ with a very small overlap $\langle-\beta_0|\beta_0\rangle$, this measurement, even with a poor resolution, will be able to discriminate between $|\pm\beta_0\rangle$.

We need hence a viable decomposition of the cross-Kerr operator $e^{i\pi\hat{n}_1\hat{n}_2}$ appearing in Eq. (38) in terms of elementary gates from the universal set. Crucially, the error with which this gate has to be implemented must lie below a fixed threshold, which is related to the desired fidelity on the resulting GKP states. As we will see, this threshold imposes constraints on how the decomposition should be performed.

Several strategies for gate decomposition are possible. In Refs. [29,30] an alternate technique to *Trotterization* is presented, referred to as *splitting*, or fractal decomposition. This method is particularly suitable when the parameter characteristic of the interaction is small, otherwise very high-order decompositions are needed (see condition (44) in Ref. [29]). Inspired by Ref. [28], we use a hybrid ad-hoc strategy that combines these two approaches, preceded by concatenation. Our decomposition is thereby structured in the following nested steps that progressively reduce the strength of the interaction applied: (1) concatenation, (2) splitting, and (3) rescaling. In the following we describe the decomposition in detail. We use a different order of presentation of the steps listed above, in order to make the presentation clearer.

1. Decomposition of the cross-Kerr interaction

a. Splitting. We aim at implementing the cross-Kerr evolution $e^{i\tau\hat{n}_1\hat{n}_2}$ to a total final precision y. In order to do so, the operator $\hat{n}_1\hat{n}_2$ defining the cross-Kerr interaction must be split in operators belonging to the set of elementary gates. First note that the cross-Kerr operator is given by

$$\begin{aligned} \hat{n}_1\hat{n}_2 &= \tfrac{1}{2}(\hat{q}^2 + \hat{p}^2 - 1)_1 \otimes \tfrac{1}{2}(\hat{q}^2 + \hat{p}^2 - 1)_2 \\ &= \tfrac{1}{4}(\hat{q}_1^2\hat{q}_2^2 + \hat{q}_1^2\hat{p}_2^2 + \hat{p}_1^2\hat{q}_2^2 + \hat{p}_1^2\hat{p}_2^2) - \tfrac{1}{4}(\hat{q}_1^2 + \hat{p}_1^2) \\ &\quad - \tfrac{1}{4}(\hat{q}_2^2 + \hat{p}_2^2) \\ &\equiv \hat{O}_1 + \hat{O}_2 + \hat{O}_3 + \hat{O}_4 - \tfrac{1}{4}(\hat{q}_1^2 + \hat{p}_1^2) - \tfrac{1}{4}(\hat{q}_2^2 + \hat{p}_2^2), \end{aligned} \tag{39}$$

where we have defined $\hat{O}_1 = \hat{q}_1^2\hat{q}_2^2/4$, $\hat{O}_2 = \hat{q}_1^2\hat{p}_2^2/4$, $\hat{O}_3 = \hat{p}_1^2\hat{q}_2^2/4$, $\hat{O}_4 = \hat{p}_1^2\hat{p}_2^2/4$. Note the operator $\hat{O}_1 + \hat{O}_2 + \hat{O}_3 + \hat{O}_4$ commutes with the product of the Fourier transforms acting on modes 1 and 2. So the cross-Kerr evolution of amplitude π reads

$$e^{i\pi\hat{n}_1\hat{n}_2} = e^{i\pi(\hat{O}_1+\hat{O}_2+\hat{O}_3+\hat{O}_4)}\hat{F}_1^\dagger\hat{F}_2^\dagger. \tag{40}$$

Therefore, we can focus on the decomposition of the operator $e^{i\pi(\hat{O}_1+\hat{O}_2+\hat{O}_3+\hat{O}_4)}$. When the parameter τ characteristic of the interaction is smaller than one, applying twice the second-order splitting $e^{i\tau(A+B)} = e^{\frac{i\tau}{2}A}e^{i\tau B}e^{\frac{i\tau}{2}A} + O(\tau^3)$ [29] gives

$$\begin{aligned} &e^{i\tau(\hat{O}_1+\hat{O}_2+\hat{O}_3+\hat{O}_4)} \\ &= e^{i\frac{\tau}{4}\hat{O}_1}e^{i\frac{\tau}{2}\hat{O}_2}e^{i\frac{\tau}{4}\hat{O}_1}e^{i\frac{\tau}{2}\hat{O}_3}e^{i\tau\hat{O}_4}e^{i\frac{\tau}{2}\hat{O}_3}e^{i\frac{\tau}{4}\hat{O}_1}e^{i\frac{\tau}{2}\hat{O}_2}e^{i\frac{\tau}{4}\hat{O}_1} \\ &\quad + \tau^3 f(\hat{O}_1, \hat{O}_2, \hat{O}_3, \hat{O}_4). \end{aligned} \tag{41}$$

b. Concatenation. Overall however, we need a strength $e^{i\pi\hat{n}_1\hat{n}_2}$ for the cross-Kerr interaction as appearing in Eq. (38). In order to achieve this, we observe that

$$e^{i\pi\hat{n}_1\hat{n}_2} = \left(e^{i\frac{\pi}{p}\hat{n}_1\hat{n}_2}\right)^p. \tag{42}$$

Identifying $\tau = \pi/p$, from Eq. (41) we see that the precision with which each step $(e^{i\frac{\pi}{p}\hat{n}_1\hat{n}_2})$ is implemented is $\tau^3 = (\pi/p)^3$. From Eq. (42), the desired gate $e^{i\pi\hat{n}_1\hat{n}_2}$ is then implemented up to precision $p\tau^3 = \pi^3/p^2$. This must equal the total desired precision y. Therefore, this allows us to fix how the number of needed iterations p depends on the precision y:

$$p = \left(\frac{\pi^3}{y}\right)^{1/2}, \tag{43}$$

yielding

$$\tau = \frac{\pi}{p} = \left(\frac{y}{\pi}\right)^{1/2}. \tag{44}$$

c. Rescaling. We now have to decompose the factors appearing in Eq. (41). From Eq. (5) of Ref. [28] we have [31]

$$\hat{p}_1^2\hat{p}_2^2 = -\tfrac{1}{9}[\hat{p}_2^3, [\hat{p}_1^3, \hat{q}_1\hat{q}_2]]. \tag{45}$$

The evolution stemming from the operator $\hat{q}_1\hat{q}_2$ belongs to our set of gates, while those corresponding to $\hat{p}_2^3$ and $\hat{p}_1^3$ can be obtained by Fourier transforming the cubic phase gate also in the set, namely $\hat{p}^3 = \hat{F}\hat{q}^3\hat{F}^\dagger$. The other terms of Eq. (39)

TABLE II. Summary of the definitions of the different fidelities between GKP states addressed in this paper. The overall distance between $|\tilde{0}_m\rangle$ and $|0_G\rangle$ is $\varepsilon_m = \zeta_m + 2^m y$. Also note that the respective encoded data qubits share the same trace distances, due to the fact that encoding consists of a unitary operation.

Approximate GKP	$\rightarrow$	Binomial GKP	$\rightarrow$	Gaussian GKP
$|\tilde{0}_m\rangle$	$2^m y$	$|0_m\rangle$	ζ_m	$|0_G\rangle$

can be obtained by Fourier transforming on one or two modes, e.g.,

$$e^{\frac{it\hat{q}_1^2\hat{q}_2^2}{4}} = \hat{F}_1^\dagger \hat{F}_2^\dagger e^{\frac{it\hat{p}_1^2\hat{p}_2^2}{4}} \hat{F}_1 \hat{F}_2. \tag{46}$$

Therefore, it is only necessary to further decompose the operator in Eq. (45), namely the evolution $e^{\frac{it\hat{p}_1^2\hat{p}_2^2}{4}} = e^{-\frac{it[\hat{p}_2^3,[\hat{p}_1^3,\hat{q}_1\hat{q}_2]]}{36}}$.

Rescaling can be carried out as done in the Supplemental Material of Ref. [28]. In Appendix A we derive the rescaling equations relevant to our purposes, in analogy to the derivation presented in Ref. [28]. We obtain

$$e^{it\tau[\hat{B},[\hat{C},\hat{A}]]} = \left[e^{i\hat{B}\frac{\tau^{1/3}}{k}} \left(e^{i\hat{A}\frac{\tau^{1/3}}{kl}} e^{i\hat{C}\frac{\tau^{1/3}}{kl}} e^{-i\hat{A}\frac{\tau^{1/3}}{kl}} e^{-i\hat{C}\frac{\tau^{1/3}}{kl}} \right)^{l^2} \right.$$
$$\left. \times \ e^{-i\hat{B}\frac{\tau^{1/3}}{k}} \left(e^{-i\hat{A}\frac{\tau^{1/3}}{kl}} e^{-i\hat{C}\frac{\tau^{1/3}}{kl}} e^{i\hat{A}\frac{\tau^{1/3}}{kl}} e^{i\hat{C}\frac{\tau^{1/3}}{kl}} \right)^{l^2} \right]^{k^3}$$
$$+ O\left(\frac{\tau^{4/3}}{k} \right) + O\left(\frac{\tau}{l} \right), \tag{47}$$

which we can now use (upon a further rescaling $\tau \rightarrow -\tau/36$) with the following identification of the operators in Eq. (45): $\hat{A} = \hat{q}_1\hat{q}_2$, $\hat{B} = \hat{p}_2^3$, and $C = \hat{p}_1^3$. Since in Eq. (41) there appear nine operators that require a decomposition of the kind in Eq. (47), in order to provide a more conservative estimate we require that each factor is implemented up to a precision $\tau^3/9$. Therefore we must require the identifications $\tau^{4/3}/(36^{4/3}k) \sim \tau^3/9$ and $\tau/(36l) \sim \tau^3/9$, which implies using Eq. (44)

$$k \sim 9^{-1/3} 4^{-4/3} \tau^{-5/3} = 9^{-1/3} 4^{-4/3} \left(\frac{y}{\pi} \right)^{-5/6},$$

$$l \sim \tau^{-2}/4 = \left(\frac{y}{\pi} \right)^{-1}/4. \tag{48}$$

We stress again that the final precision y on the cat state generation affects the quality of the binomial GKP states that are generated with this protocol. More precisely, since a binomial GKP state of order m requires 2^m cat states, the error y is amplified accordingly: for a given m, the distance between the approximate GKP states generated through this procedure and the binomial GKP states is upper bounded by $2^m y$. We indicate the approximate binomial GKP states by $|\tilde{0}_m\rangle$. A summary of the fidelities between different GKP states is provided in Table II.

To summarize, we have provided a decomposition of the cross-Kerr interaction $e^{i\pi\hat{n}_1\hat{n}_2}$ in gates of the form $e^{ib\hat{q}_1\hat{q}_2}$, $e^{ic\hat{q}^3}$, $e^{ig(\hat{q}\hat{p}+\hat{p}\hat{q})}$, $\hat{F}$. In Appendix B we provide an estimate of the scaling of the required number of gates in order to achieve a precision of y, which results in $N \propto y^{-3}$. This results in particular in a roughly a thousand elementary gates for a required precision of 0.1 in the cross-Kerr gate implementation.

What we further have to do is to provide a decomposition of the squeezing gate $e^{ig(\hat{q}\hat{p}+\hat{p}\hat{q})}$ in terms of the elementary gates of Eqs. (7) and (8). Also, in the procedure outlined above for the GKP synthesis from cat states a beam splitter appears. Therefore we must also decompose this transformation into elementary gates. This is the goal of the next subsection.

2. Decomposition of beam splitters and squeezers

In order to cast the gates used for the cross-Kerr evolution in the form admitted by the set A_1 supplemented by the Fourier transform, we have to provide an expression of the squeezing operator and of the beam splitter in terms of $\hat{q}$-diagonal gates and Fourier transforms. In contrast to the decomposition of the previous subsection, these can be provided exactly. We show the detailed calculation in Appendix C. The result is the following: the squeezing operator is decomposed onto

$$e^{-i\frac{\ln s}{2}(\hat{q}\hat{p}+\hat{p}\hat{q})} = \hat{F} e^{\frac{is\hat{q}^2}{2}} \hat{F} e^{\frac{i\hat{q}^2}{2s}} \hat{F} e^{\frac{is\hat{q}^2}{2}}, \tag{49}$$

while the beam splitter operator decomposes as

$$\hat{F}\hat{O}(q)\hat{F}\hat{O}(q)\hat{F}\hat{O}(q), \tag{50}$$

with $\hat{O}(q) = e^{i\frac{1}{2\sqrt{2}}(\hat{q}_1^2 - \hat{q}_2^2 + \hat{q}_1\hat{q}_2)}$. Note that in turn $O(\hat{q})$ can be trivially decomposed into shear and $\hat{C}_Z$ gates. Now all the gates necessary to implement an approximate GKP state have been decomposed onto gates of the elementary set Eqs. (7) and (8).

V. NOISE IN CV AND FAULT TOLERANCE

Fault tolerance in CV is an issue that must be addressed specifically. In this section we show that the universal model defined in Sec. III A can be made fault tolerant.

In CV, the natural basis for quantum channels consists of all possible displacement operators. Formally, a general noise model $\mathcal{E}$ on an arbitrary input state $\hat{\rho}$ can be expanded in terms of shifts acting on $\hat{\rho}$, according to the following expression [17]:

$$\mathcal{E}(\hat{\rho}) = \int du \, dv \, du' \, dv' \, C(u,v,u',v') e^{-iu\hat{p}} e^{-iv\hat{q}} \hat{\rho} \, e^{iv'\hat{q}} e^{iu'\hat{p}}, \tag{51}$$

where $\mathcal{E}$ is completely positive and trace preserving. Therefore an error-correcting procedure in CV applies to arbitrary noise models if it allows one to correct for arbitrary displacement errors (similar to qubits where an arbitrary error can be corrected based on Pauli-error correction), which intuitively is possible when the support of the error distribution C is concentrated on sufficiently small values. This feature is enabled by the GKP encoding [17] using an additional source of ancillary GKP $|0_G\rangle$ states, where as we have already noted the notation $|0_G\rangle$ indicates that the ancillary GKP states employed are the Gaussian ones, i.e., enveloped by a Gaussian and correspondingly associated with a finite squeezing degree. The specific circuit for error correction is shown in Fig. 5.

The noise reduction (i.e., error correction in the CV sense) works if the measurement on the ancillary mode yields the correct $\sqrt{\pi}$-long interval on the real axis. The displacement error acting on the data qubit in one of the quadratures is then replaced by the independent error coming from the fresh

ancillary GKP state. Repeating the procedure after a Fourier transform ensures that the displacement errors in both quadratures are replaced. To summarize, this probabilistic procedure ensures that the CV noise remains controlled and determined by the noise linked to the supply of GKP states. The failure probability itself is determined by how likely the noise is to displace the state by more than $\sqrt{\pi}/2$.

An important step was taken in [18], where the authors combined this noise reduction procedure with an additional layer of qubit error-correcting code at the logical encoding level. They showed that if the procedure fails—that is the measured displacement error was larger than $\sqrt{\pi}/2$—the controlled-displacement actually corresponds to a bit flip at the GKP encoding level. Then one can use a standard qubit error-correcting code to address this bit flip error. This ensures that the failure probability of the procedure, as soon as it is lower than the threshold associated with the qubit error-correcting code, can be made arbitrarily small, thus enabling fault tolerance for a CV hardware. Note that the squeezing level required in order to fulfill the threshold condition according to the procedure described above can be lowered by utilizing a more refined error-correction scheme [32]. The latter exploits a priori information stemming from the Gaussian distribution in each GKP peak together with the analog information associated with the syndrome detections, rather than only using binary information corresponding to the measured displacement being "inside" or "outside" the above mentioned $\sqrt{\pi}$-long interval. This method also allows for the reduction of the number of the concatenation steps in a full error-correcting procedure [33]. For the purpose of keeping our discussion less technical, however, we will refer to the original error-correction scheme of Ref. [18] in order to derive bounds on the squeezing level as well as other parameters for our model.

There may be numerous origins for this CV noise: usually not only the "data qubit" will be noisy, but the ancillary one and the measurement (e.g., finite resolution) will also. Crucially the characteristics of the noise do not really matter. The only relevant questions are: what is the probability that all these errors put together yield a displacement larger than $\sqrt{\pi}/2$? Is it possible to make this probability lower than the threshold of some qubit error-correcting code $\varepsilon_{\rm th}$? Mathematically, we aim to analyze and upper bound the following probability:

$$\Pr\left(|p| > \frac{\sqrt{\pi}}{2}\right), \tag{52}$$

where p is the displacement error measured in the protocol shown in Fig. 5. However this probability may turn out to be too difficult to compute. We show in the following how
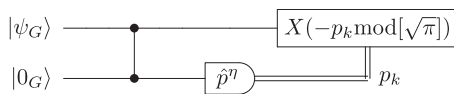

FIG. 5. Procedure to correct for errors in the $\hat{q}$ quadrature. $|\psi\rangle$ is the data qubit and $|0_G\rangle$ is a Gaussian GKP state. After measurement on the second mode the result p_k is used to shift the first mode back.

to reduce this problem to a much simpler one only involving Gaussian functions.

We are going to assume GKP encoding as explained above. The data qubit is, however, encoded in the approximate GKP states basis obtained with the procedure outlined in Sec. IV. We denote the corresponding density matrix with $\tilde{\rho}_m$. When noise enters the picture the output state ρ can be a mixed state. We characterize the noise model by a parameter ε which upper bounds the distance:

$$d(\rho, \tilde{\rho}_m) \equiv \frac{1}{2}||\rho - \tilde{\rho}_m|| < \varepsilon, \tag{53}$$

where $||\cdot||$ indicates the standard trace norm. Similarly we can upper bound the distance between the approximate GKP states and the standard Gaussian GKP states $|0/1_G\rangle$. Recall that it is determined by two contributions: ζ_m coming from the imperfect fidelity between the binomial GKP states and the Gaussian GKP states—see Table I, Table II, and Eq. (19); and $2^m y$ because of the approximate procedure used to generate Schrödinger cat states and thus approximate GKP states, stemming from finite precision gates—see the discussion following Eq. (48). Sticking with the density matrix formalism for consistency, we denote as ρ_G the closest Gaussian GKP-encoded state to the corresponding approximate GKP-encoded state $\tilde{\rho}_m$:

$$d(\tilde{\rho}_m, \rho_G) < \varepsilon_m, \tag{54}$$

where $\varepsilon_m = \zeta_m + 2^m y$.

Suppose now that one wishes to reduce the noise of a state ρ using the procedure described in Fig. 5. There the input state is $\rho_G|0_G\rangle\langle 0_G|$, where the tensor product is implicit. In our scheme, the input state is replaced by $\rho|\tilde{0}_m\rangle\langle\tilde{0}_m|$, where $|\tilde{0}_m\rangle$ is the logical 0 state encoded in the approximate GKP basis. We focus first on the trace distance for the joint state after the C_Z gate shown in Fig. 5. For a perfect, unitary C_Z gate and using properties of the trace norm we have

$$d(C_Z\rho|\tilde{0}_m\rangle\langle\tilde{0}_m|C_Z^\dagger, C_Z\rho_G|0_G\rangle\langle 0_G|C_Z^\dagger)$$

$$= d(\rho|\tilde{0}_m\rangle\langle\tilde{0}_m|, \rho_G|0_G\rangle\langle 0_G|)$$

$$\leqslant d(\rho|\tilde{0}_m\rangle\langle\tilde{0}_m|, \tilde{\rho}_m|\tilde{0}_m\rangle\langle\tilde{0}_m|) + d(\tilde{\rho}_m|\tilde{0}_m\rangle\langle\tilde{0}_m|, \rho_G|\tilde{0}_m\rangle\langle\tilde{0}_m|)$$

$$+ d(\rho_G|\tilde{0}_m\rangle\langle\tilde{0}_m|, \rho_G|0_G\rangle\langle 0_G|)$$

$$< \varepsilon + \varepsilon_m + \varepsilon_m. \tag{55}$$

In other words, the statistical distance for the noise reduction protocol using approximate GKP states as ancillary qubits compared to using Gaussian GKP states is upper bounded by $\varepsilon + 2\varepsilon_m$. Hence the possible deviations of the measurement results are also upper bounded by $\varepsilon + 2\varepsilon_m$.

We now define p (p_G) as the measured displacements in the (Gaussian) protocol. Equation (55) implies that $|p - p_G| < \varepsilon + 2\varepsilon_m$. Let us consider now the failure probability that we wish to upper bound, that is

$$P_{\rm fail} = \Pr(|p| > \sqrt{\pi}) = \Pr\left(|p - p_G + p_G| > \frac{\sqrt{\pi}}{2}\right)$$

$$\leqslant \Pr\left(|p_G| + |p - p_G| > \frac{\sqrt{\pi}}{2}\right)$$

$$\leqslant \Pr\left(|p_G| > \frac{\sqrt{\pi}}{2} - |p - p_G|\right)$$

$$\leqslant \Pr\left(|p_G| > \frac{\sqrt{\pi}}{2} - (\varepsilon + 2\varepsilon_m)\right). \tag{56}$$

In other words, if we aim to upper bound the probability that our error-correction protocol fails—and show that it can be made lower than some threshold probability ε_{th}—we simply have to consider the Gaussian protocol using $\sqrt{\pi}/2 - (\varepsilon + 2\varepsilon_m)$ as a bound rather than $\sqrt{\pi}/2$.

Recall finally that the protocol actually needs to be repeated after a Fourier transform to correct for the noise in both quadratures. The protocol is successful if both rounds are, i.e., the total failure probability can be expressed as

$$1 - P_{\text{succ}_1} P_{\text{succ}_2} = 1 - (1 - P_{\text{fail}_1})(1 - P_{\text{fail}_2}), \tag{57}$$

where 1 and 2 refer to error-correction rounds on the two respective quadratures. For real σ and δ we denote $\chi(\sigma, \delta) = \Pr(|p_G(\sigma)| > \sqrt{\pi}/2 - \delta)$, where we stress that p_G actually depends on the squeezing σ of the Gaussian GKP states. A given noise model corresponds to nonvanishing values for the distances ε and ε_m. Then, combining Eqs. (56) and (57), the fault tolerance condition amounts to finding a squeezing parameter σ_{th} such that the following bound on the total failure probability holds:

$$1 - [1 - \chi(\sigma_{\text{th}}, \varepsilon_q + 2\varepsilon_m)][1 - \chi(\sigma_{\text{th}}, \varepsilon_p + 2\varepsilon_m)] < \varepsilon_{\text{th}}. \tag{58}$$

Note that in principle the Fourier transform in between the two rounds of noise reduction may disturb the system and thus yield a different upper bound for the trace distance, hence the notation $\varepsilon_{1,2}$, e.g., the measurement based implementation of the Fourier transform (see, e.g., the Supplemental Material of Ref. [19] for a detailed discussion).

To summarize, we have shown how to reduce an arbitrary noise model to simply considering Gaussian GKP states with slightly modified thresholds. This allows one to easily compute the relevant probabilities since they now only consist of integrating tails of Gaussian functions.

VI. CONSEQUENCES FOR THE CV GATES

In this section we determine the conditions that fault tolerance requirements impose on the gate parameters defined in Sec. III Eqs. (7) and (10). These also depend on the precision of the gate decomposition that we derived in the previous sections.

A. Universal computational model

The results detailed in Sec. V pave the way for fault tolerance: whatever noise model one has to deal with, it can be plugged in our computational model to be translated into specific requirements for the gate parameters and still allow for error correction.

Here we find instructive to discuss the case given in the abstract definition of our computational model introduced in Sec. III A, where the gates belonging to the model are
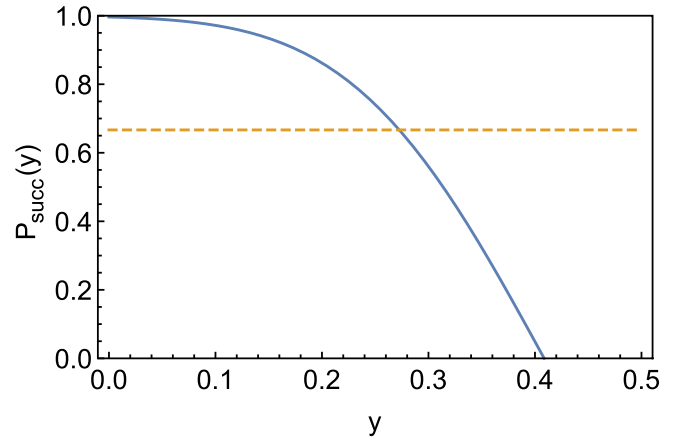

FIG. 6. Success probability P_{succ} in Eq. (61) as a function of y (solid line). As a guide for the eye, the reference level 2/3 is also plotted (dashed line).

assumed to be perfectly implemented, i.e., there are no external sources of error. This corresponds to setting $\varepsilon_q = \varepsilon_p = 0$ and no active error correction is required. However, using approximate GKP states for logical information encoding yields an intrinsic error probability. Following the analysis performed in [17], this probability can be linked to the integrals of Gaussian functions, i.e., to the error function. For a Gaussian GKP state of symmetric squeezing parameter σ it simply reads $\text{erf}(\sqrt{\pi}/2\sigma)$, where erf denotes the error function. In our case this probability also depends on the ε_m defined in Eq. (54), as well as on the gate parameters required for universal quantum computing. Namely, we have

$$P_{\text{succ}}(m, y) = \text{erf}\left(\frac{\frac{\sqrt{\pi}}{2} - \varepsilon_m}{\sigma}\right), \tag{59}$$

where m and σ are related according to the discussion in Sec. IV, and where in particular ε_m depends on the precision y.

We consider the experimentally easiest case where $m = 1$, so $\varepsilon_1 = \zeta_1 + 2y$. Given the analysis performed in Sec. IV, the corresponding approximate GKP states can be compared to Gaussian GKP states with a squeezing parameter of 5 dB. The associated fidelity shown in Table I can be used to estimate ζ_1:

$$\zeta_1 \leqslant \sqrt{1 - 0.9976^2} \approx 0.069. \tag{60}$$

In order to compute the corresponding gate parameters, we plot in Fig. 6 the success probability P_{succ} as a function of the errors y in the implementation of the cross-Kerr interaction discussed in Sec. IV. It reads

$$P_{\text{succ}}(y) = \text{erf}\left(\frac{\frac{\sqrt{\pi}}{2} - \zeta_1 - 2y}{\sigma}\right). \tag{61}$$

To a value of the gate precision of $y = 0.1$ corresponds a success probability of approximately 0.97. Therefore in the following we will use this value to derive the corresponding gate parameters and understand the experimental consequences.

Based on the requirement of $y = 0.1$ and $m = 1$, we can now compute the gate parameters corresponding to the gate

TABLE III. Summary of the parameters for the definition of the gates of the universal model and of the CV random sampling model Eqs. (7) and (8), based on a precision of $y = 0.1$ and $m = 1$.

Evolution	GKP generation step	Parameters
Displacement	Coherent state initialization	$d \simeq 5.6$
Shearing	Squeezing of the cat	$s_1 \simeq 0.73$; $s_2 \simeq 1.1$
Entanglement	Beam splitter	$b_1 \simeq 0.35$
	Cross-Kerr decomposition	$b_2 \simeq 0.011$
Cubic	Cross-Kerr decomposition	$c_1 \simeq 0.011$
		$c_2 \simeq 0.086$

set A_1 defined in Sec. III A Eq. (7). As drawn from the previous sections, using in particular Eqs. (47) and (49) we obtain the numerical values summarized in Table III. Together with the gates required to implement the beam splitter appearing in Eq. (50), this completes the set of gates that defines our model.

B. Subuniversal models

In this section we provide a proof of classical computational hardness of exact sampling in the worst-case scenario for both subuniversal models introduced in Sec. III B. First we focus on the circuit illustrated in Fig. 2, and argue that its hardness directly follows as a consequence of the universality of the model of computation that we have addressed in Sec. VI A. Then we turn to CVIQP (Fig. 3), and refine the proof that was provided in Ref. [19] by dropping the requirement of input GKP states. To achieve this goal, we use similar arguments to those that allowed us to claim fault tolerance in the probabilistic universal model presented above. As we shall see, the required constraints are tighter for the CVIQP model.

1. CV random circuit sampling is hard

The first circuit that we address is shown in Fig. 2, corresponding to picking gates randomly from the sets that define the probabilistic universal computational model discussed in the previous Sec. VI A. For the case of exact sampling, a very standard proof of classical hardness can be provided [19,34–36]. In general, if a subuniversal computational model of quantum computation becomes universal when post-selecting on a subset of the outputs—i.e., contains the class postBQP—, then information-theoretic arguments allow one to conclude that efficient classical simulation of this subuniversal model is impossible. These arguments are based on widely held conjectures of classical complexity theory, like the so-called polynomial hierarchy not collapsing. Hence the main point that we have to show is that post-selection makes the circuit of Fig. 2 as powerful as postBQP.

This statement directly follows from the universality of the model presented in Sec. VI A. As we have shown in Sec. IV, the gates in Eq. (7) allow for the probabilistic generation of approximate GKP states with success probability given by Eq. (29). Crucially, the fact that the success probability is exponentially low in the number of approximate GKP states that need to be produced does not hinder this result [37]. Therefore, any quantum circuit can be run probabilistically

using elements drawn only from the family of circuits of Fig. 2. Then post-selecting on successfully passing these probabilistic events yields the correct computation. Furthermore, one can also post-select on an additional subset of the outputs. It means that universal and post-selected quantum computations, i.e., postBQP, can be performed using circuits of the type described in Fig. 2.

We also stress that post-selection should be regarded as a mathematical trick for the proof of hardness, and that experimentally probing the model under consideration would just consist of sampling from an architecture belonging to the family depicted in Fig. 2, with no actual need for practical post-selection on measurement outcomes, nor for actual generation of GKP states.

2. CVIQP with input squeezed states is hard

The second circuit family we address is sketched in Fig. 3. In order to show that the model CVIQP is hard to sample classically, we build on the proof presented in [19], which was established for an analogous model, but with Gaussian GKP states available at the input. The squeezing parameter of those GKP states, furthermore, was required to scale logarithmically with the circuit size, namely we had

$$\sigma \propto \log n, \qquad (62)$$

where σ in dB characterizes the widths of the Gaussian describing the GKP state wave function and n is the number of modes. Just like for the model addressed in Sec. VI B 1, the main structure of reasoning to claim computational hardness was based on showing that the class defined as postCVIQP, i.e., CVIQP with the additional resource of post-selection, is as powerful as postBQP. In other words, postCVIQP is a universal and fault-tolerant model of QC—supplemented with post-selection.

In order to obtain universality and fault tolerance in the post-selected model (i.e., to show that it is as powerful as postBQP), we first show that the condition (62) is actually unnecessary for the hardness statement of Ref. [19] to hold, and that a constant σ is sufficient to prove the hardness of the circuit. Furthermore, note that the GKP state generation can be subsumed in the circuit model definition when this is augmented with post-selection, similarly as we did in Sec. VI B 1. Then we analyze the bound on the input squeezing imposed by the fault tolerance requirement of the model with post-selection.

The probability of a successful post-selection only makes sense if it is not worse than exponentially low, which in particular is guaranteed by the scaling law for the squeezing parameter derived in [19]. However, the post-selection happens at a logical, encoding level so it actually corresponds to several physical measurement outcomes recombined according to the error-correcting code. Each of these outcomes is noisy because of the CV nature of the quantum states, which can be understood as encoding imperfect, nonorthogonal qubits. However, the threshold theorem states that the probability of reaching a wrong conclusion at the encoding level can be made exponentially low since the physical noise can be mapped to a qubit error following the procedure described in the previous section.
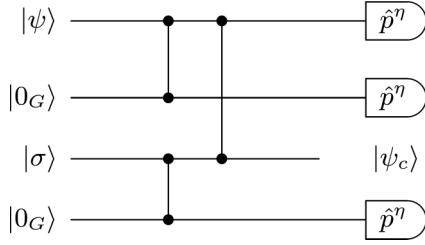
FIG. 7. Circuit implementation of an error-corrected Fourier transform based on the resources available in the CVIQP model, where $|\psi_c\rangle$ denotes the output corrected state.

TABLE IV. Summary of the parameters for the definition of the gates of the CVIQP model, based on a precision of $y = 10^{-3}$ and $m = 6$.

Evolution	GKP generation step	Parameters
Displacement	Coherent state initialization	$\tilde{d} \simeq 142$
Shearing	Squeezing of the cat	$\tilde{s}_1 \simeq 0.28; \tilde{s}_2 \simeq 0.89$
Entanglement	Beam splitter	$\tilde{b}_1 \simeq 0.35$
	Cross-Kerr decomposition	$\tilde{b}_2 \simeq 1.6 \times 10^{-6}$
Cubic	Cross-Kerr decomposition	$\tilde{c}_1 \simeq 1.6 \times 10^{-6}$
		$\tilde{c}_2 \simeq 1.3 \times 10^{-3}$

More specifically, this mapping is ensured by the use of GKP states, and by associating the measurement outcomes of the homodyne detection in given intervals to either 0 or 1 at the logical level. For a symmetric Gaussian noise, an upper bound as a function of the squeezing can be found in [17] with additional approximations. Therefore, the scaling condition in Eq. (62) was actually unnecessary.

Now, recall that the proof of hardness for CVIQP circuits holds if we can make sure that postCVIQP circuits are able to realize universal quantum computations. However, since the Fourier transform does not belong to the computational model defined by CVIQP circuits, it can only be implemented in postCVIQP using a measurement-based approach as shown in Fig. 7. This approach unfortunately introduces additional noise, which implies that we have to rely on quantum error correction for CV quantum computation as discussed in Sec. V.

The Fourier transform can be implemented in a single, post-selected, teleportation step. The squeezing parameter σ characterizing the squeezed vacuum state is added to the variance of the momentum quadrature of the state being teleported. Based on the analyses developed in Sec. V and Ref. [18] and neglecting the effects of finite resolution, a sufficient condition to achieve fault tolerance can be derived, similar to the one in Eq. (58), and it reads

$$1 - (1 - \chi(\sqrt{2}\sigma, 2\varepsilon_m))(1 - \chi(\sqrt{5}\sigma, 2\varepsilon_m)) < \varepsilon_{\text{th}}, \quad (63)$$

for a given qubit error-correcting code of threshold probability ε_{th}.

We chose the lowest value of m compatible with Eq. (63). For a threshold probability $\varepsilon_{\text{th}} = 10^{-6}$ we find that $m = 6$, which corresponds to a squeezing of 19 dB according to Eq. (16), is the minimal amount of squeezing that satisfies Eq. (63). It yields an upper bound on $\varepsilon_6 \approx 0.05$. Recall that $\varepsilon_6 = 2^6 y + \zeta_6$. Using Eq. (19) we have $\zeta_6 \approx 3 \times 10^{-3}$ so we get an upper bound for the error rate in the Schrödinger cat states generation of

$$y \leqslant 10^{-3}. \quad (64)$$

This value constitutes a much stronger requirement than the value of 10^{-1} found in Sec. VI A when discussing the model for universal quantum computing. It stems from the fact that the set of gates in CVIQP circuits does not include the Fourier transform, which must be implemented in a measurement-based fashion entailing an additional error due to finite squeezing in the ancillary squeezed state. Analogous

to what we found for the universal model in Table III, this value of precision allows for the derivation of corresponding gate parameters for the definition of the CVIQP model of Eq. (10). These parameters are shown in Table IV.

In conclusion to this section on subuniversal models, we stress that neither for the CV random circuit sampling model discussed in Sec. VI B 1 nor for CVIQP an actual generation of GKP states is needed in practice: the statement on computational hardness holds for sampling from the output probability distributions of the circuits in Figs. 2 and 3, respectively. In contrast to the universal model, GKP generation and encoding was only used as a conceptual intermediate step for the proof of hardness.

VII. CONCLUSIONS

In summary, we have derived what is to our knowledge the first quantum computational model in CV based only on input vacuum states, and we have shown that a finite set of gates and homodyne detection are sufficient to achieve probabilistic universal QC and fault tolerance. This model can be adapted to yield sampling problems which are hard to sample for classical computers unless the polynomial hierarchy collapses. These consist of a CV random circuit sampling model with the same structure as for universal computations and a model analogous to IQP for qubits based on momentum squeezed vacuum states (CVIQP).

Regarding fault tolerance, in the universal model the gates are implemented perfectly, and no active correction is required. However, the intrinsic noise inherent to approximate GKP states can be linked to the parameters of the gates defining our model, allowing us to determine the value of the gate parameters to use. Consistently with those gate parameters, GKP states generated from two Schrödinger cat states only can be used, which is experimentally not too demanding. The hardness proof for the CV random circuit model, which is directly based upon the basis of the universal model, relies on similar considerations.

On the other hand, for the CVIQP model, more stringent requirements on fault tolerance are imposed by the fact that the Fourier transform does not belong to the gate set. Correspondingly, stronger constraints on the squeezing parameter and gate precision arise.

A candidate platform where proof-of-principle experiments of the present models could be addressed is provided by optical systems, where spontaneous parametric downconversion allows for the generation of multimode squeezed states of

light [38,39] that can be subsequently manipulated and, e.g., entangled in large cluster states [40–42]. In these systems, engineering nonlinearities necessary for the implementation of cubic gates is challenging. Attempts to probabilistically achieve this aim have been performed by means, e.g., of photon subtraction [43] and more generally with the use of single photon detectors [44,45], towards the implementation of a full cubic-phase gate with photon counters [17,46]. More recently, microwave radiation coupled to superconducting qubits has proven useful for the generation of squeezed states [2,47]. In this promising setup, nonlinearities allowing for the generation of non-Gaussian states can be provided by the coupling with superconducting Josephson junctions, acting as artificial atoms on the microwave field [48]. Finally, optomechanical systems are also promising candidates for the generation of multimode squeezed and cluster states of radiation [5]. There, non-Gaussian states could also be deterministically generated [49].

We believe our work opens up new perspectives. Concerning the universal model, several aspects can be further optimized, from the gate decomposition [29] of the cross-Kerr implementation to the error-correcting procedure [50]. A further way to drastically reduce the number of gates necessary for the implementation of the cross-Kerr interaction could be to include in the elementary gates set a quartic Hamiltonian $e^{is\hat{q}^4}$ [51].

Furthermore, it would be interesting to study specific implementations of the gates that compose our model. For instance, in Ref. [52] a protocol was given, allowing for the implementation of polynomial approximation of arbitrary-order operations diagonal in the $\hat{q}$ quadrature (including non-Gaussian operations), with the use of ancillary photon-subtracted squeezed states. Merging the two approaches, upon proper considerations on error-probability and fault tolerance specific to the gate implementation considered, would result in probabilistic fault-tolerant universal QC from photon subtracted squeezed states and Gaussian operations as building blocks. As for the sampling models considered, it would be desirable to extend the hardness proof to the average case, and to the approximate sampling case.

APPENDIX A: NESTED COMMUTATORS USED FOR THE RESCALING STEP

The starting point is

$$e^{t^2[\hat{B},\hat{A}]} = e^{it\hat{B}}e^{it\hat{A}}e^{-it\hat{B}}e^{-it\hat{A}} + O(t^3, \hat{A}, \hat{B}). \quad \text{(A1)}$$

Now using the identity $e^{t^2[\hat{B},\hat{A}]} = e^{(\frac{t}{n})^2[\hat{B},\hat{A}]n^2}$ and using Eq. (A1) with $t \to t/n$ we obtain

$$e^{t^2[\hat{B},\hat{A}]} = \left[e^{i\frac{t}{n}\hat{B}}e^{i\frac{t}{n}\hat{A}}e^{-i\frac{t}{n}\hat{B}}e^{-i\frac{t}{n}\hat{A}} + O\left(\frac{t^3}{n^3}, \hat{A}, \hat{B}\right) \right]^{n^2}$$

$$= \left(e^{i\frac{t}{n}\hat{B}}e^{i\frac{t}{n}\hat{A}}e^{-i\frac{t}{n}\hat{B}}e^{-i\frac{t}{n}\hat{A}} \right)^{n^2} + O\left(\frac{t^3}{n}, \hat{A}, \hat{B}\right). \quad \text{(A2)}$$

The standard equation for the nested commutator is then derived by replacing in Eq. (A1) $it\hat{A} \to t^2[\hat{B},\hat{A}]$. We then obtain

$$e^{it^3[\hat{B},[\hat{B},\hat{A}]]} = e^{it\hat{B}}e^{t^2[\hat{B},\hat{A}]}e^{-it\hat{B}}e^{-t^2[\hat{B},\hat{A}]} + O(t^4, \hat{A}, \hat{B}). \quad \text{(A3)}$$

Similarly as done before, we now use the identity $e^{it^3[\hat{B},[\hat{B},\hat{A}]]} = e^{i(\frac{t}{k})^3[\hat{B},[\hat{B},\hat{A}]]k^3}$ so that we obtain

$$e^{it^3[\hat{B},[\hat{B},\hat{A}]]} = \left(e^{i\frac{t}{k}\hat{B}}e^{\left(\frac{t}{k}\right)^2[\hat{B},\hat{A}]}e^{-i\frac{t}{k}\hat{B}}e^{-\left(\frac{t}{k}\right)^2[\hat{B},\hat{A}]} \right)^{k^3}$$

$$+ O\left(\frac{t^4}{k}, \hat{A}, \hat{B}\right). \quad \text{(A4)}$$

Now finally we replace Eq. (A2) in Eq. (A4), but with $t \to t/k$, i.e., we use $e^{(\frac{t}{k})^2[\hat{B},\hat{A}]} = e^{(\frac{t}{kl})^2[\hat{B},\hat{A}]l^2}$, yielding

$$e^{it^3[\hat{B},[\hat{B},\hat{A}]]} = \left[e^{i\hat{B}\frac{t}{k}} \left(e^{i\hat{A}\frac{t}{kl}}e^{i\hat{B}\frac{t}{kl}}e^{-i\hat{A}\frac{t}{kl}}e^{-i\hat{B}\frac{t}{kl}} \right)^{l^2} \right.$$

$$\left. \times \; e^{-i\hat{B}\frac{t}{k}} \left(e^{-i\hat{A}\frac{t}{kl}}e^{-i\hat{B}\frac{t}{kl}}e^{i\hat{A}\frac{t}{kl}}e^{i\hat{B}\frac{t}{kl}} \right)^{l^2} \right]^{k^3}$$

$$+ O\left(\frac{t^4}{k}\right) + O\left(\frac{t^3}{l}\right). \quad \text{(A5)}$$

By using the substitution $it\hat{A} \to t^2[\hat{C},\hat{A}]$ it is also possible analogously to derive

$$e^{it^3[\hat{B},[\hat{C},\hat{A}]]} = \left(e^{i\frac{t}{k}\hat{B}}e^{(\frac{t}{k})^2[\hat{C},\hat{A}]}e^{-i\frac{t}{k}\hat{B}}e^{-(\frac{t}{k})^2[\hat{C},\hat{A}]} \right)^{k^3}$$

$$+ O\left(\frac{t^4}{k}, \hat{A}, \hat{B}, C\right) \quad \text{(A6)}$$

and finally

$$e^{it^3[\hat{B},[\hat{C},\hat{A}]]} = \left[e^{i\hat{B}\frac{t}{k}} \left(e^{i\hat{A}\frac{t}{kl}}e^{i\hat{C}\frac{t}{kl}}e^{-i\hat{A}\frac{t}{kl}}e^{-i\hat{C}\frac{t}{kl}} \right)^{l^2} \right.$$

$$\left. \times \; e^{-i\hat{B}\frac{t}{k}} \left(e^{-i\hat{A}\frac{t}{kl}}e^{-i\hat{C}\frac{t}{kl}}e^{i\hat{A}\frac{t}{kl}}e^{i\hat{C}\frac{t}{kl}} \right)^{l^2} \right]^{k^3}$$

$$+ O\left(\frac{t^4}{k}\right) + O\left(\frac{t^3}{l}\right), \quad \text{(A7)}$$

which we will need in the following. Setting $\tau = t^3$ we finally obtain Eq. (47).

APPENDIX B: ROUGH ESTIMATE OF THE NUMBER OF OPERATIONS NEEDED TO IMPLEMENT THE CROSS-KERR EVOLUTION

We estimate the order of magnitude of the number of operations that are needed to implement the cross-Kerr evolution given a desired precision y. To provide an estimate, let us first focus on the term $e^{\frac{it\hat{p}_1^2\hat{p}_2^2}{4}}$. Neglecting the Fourier transforms required to implement $\hat{p}_1^3$ and $\hat{p}_2^3$ from the corresponding

position-diagonal operators, we obtain that in order to implement the nested commutator in Eq. (45) according to Eq. (47) we need

$$N_{\tau \hat{p}_1^2 \hat{p}_2^2/4} = [2(4l^2 + 1)]k^3 \sim y^{-9/2} \frac{\pi^{9/2}}{18 \times 4^4} \quad (B1)$$

elementary operations, where we have only kept the dominant term in $1/y$. From Eq. (41) we need nine of these kind of gates, with similar decompositions to $e^{\frac{i\tau \hat{p}_1^2 \hat{p}_2^2}{4}}$, in order to implement the operator $(e^{i\frac{\pi}{p} \hat{n}_1 \hat{n}_2})^p$. Finally, from Eq. (42) we see that we need to repeat p times these gates. Therefore the total number of gates necessary to implement the cross-Kerr evolution is

$$N_{\pi \hat{n}_1^2 \hat{n}_2^2} = 9 N_{\tau \hat{p}_1^2 \hat{p}_2^2/4} \; p \sim y^{-5} \frac{\pi^{3/2}}{2 \times 4^4}, \quad (B2)$$

which results in a thousand gates for $y = 0.1$.

APPENDIX C: DECOMPOSITION OF SQUEEZING AND BEAM SPLITTER IN ELEMENTARY GATES

For this analysis we find it simpler to use the symplectic formalism for the elementary gates as introduced in [53]. In this framework, the relevant gates are represented in terms of their action on the quadrature operators as (using the convention $\Delta^2 q_0 = 1/2$ for the vacuum fluctuations)

Squeezing $e^{-i\frac{\ln s}{2}(\hat{q}\hat{p}+\hat{p}\hat{q})} \rightarrow \begin{pmatrix} \hat{q}' \\ \hat{p}' \end{pmatrix} = \begin{pmatrix} s & 0 \\ 0 & 1/s \end{pmatrix} \begin{pmatrix} \hat{q} \\ \hat{p} \end{pmatrix}$,

Rotation $e^{i\frac{\theta}{2}(\hat{q}^2+\hat{p}^2)} \rightarrow \begin{pmatrix} \hat{q}' \\ \hat{p}' \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} \hat{q} \\ \hat{p} \end{pmatrix}$,

Shear $e^{\frac{is q^2}{2}} \rightarrow \begin{pmatrix} \hat{q}' \\ \hat{p}' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix} \begin{pmatrix} \hat{q} \\ \hat{p} \end{pmatrix}$,

FT $e^{\frac{i\pi}{4}(\hat{q}^2+\hat{p}^2)} \rightarrow \begin{pmatrix} \hat{q}' \\ \hat{p}' \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \hat{q} \\ \hat{p} \end{pmatrix}$. (C1)

1. Decomposition of the squeezing operator (exact)

We start with the squeezing gate. It is easy to show that

$$\begin{pmatrix} s & 0 \\ 0 & \frac{1}{s} \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ s_3 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$
$$\times \begin{pmatrix} 1 & 0 \\ s_2 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ s_1 & 1 \end{pmatrix}, \quad (C2)$$

with $s_1 = s$, $s_2 = 1/s$, $s_3 = s$. Hence using Eq. (C1) we obtain Eq. (49) of the main text.

2. Decomposition of the beam splitter operation (exact)

In the proposal of Ref. [23], squeezed cat states undergo a beam splitter transformation that is described by the symplectic matrix

$$\begin{pmatrix} q_1' \\ q_2' \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} q_1 \\ q_2 \end{pmatrix}. \quad (C3)$$

We want to decompose this beam splitter gate in terms of elementary gates. We use a procedure inspired by Ref. [54].

For the general change of basis

$$\begin{pmatrix} q_1' \\ q_2' \end{pmatrix} = \begin{pmatrix} \sqrt{R} & \sqrt{1-R} \\ \sqrt{1-R} & -\sqrt{R} \end{pmatrix} \begin{pmatrix} q_1 \\ q_2 \end{pmatrix} \equiv M_R \begin{pmatrix} q_1 \\ q_2 \end{pmatrix} \quad (C4)$$

(where the obvious identification $R = 1/2$ allows us to retrieve the case of interest of the aforementioned beam splitter) one has the identity

$$\begin{pmatrix} M_R & 0 \\ 0 & M_R \end{pmatrix} = \left[\begin{pmatrix} 0 & -I_2 \\ I_2 & 0 \end{pmatrix} \begin{pmatrix} I_2 & 0 \\ M_R & I_2 \end{pmatrix} \right]^3. \quad (C5)$$

This allows us to decompose the beam splitter into Fourier transform and a gate corresponding to $O(\hat{q}) = e^{i(b_1 \hat{q}_1^2 + b_2 \hat{q}_2^2 + b_3 \hat{q}_1 \hat{q}_2)}$. To discover the correspondence between the coefficients b_1, b_2, b_3 and R we inspect the explicit action of the operator $O(\hat{q})$ on the quadratures:

$$e^{-i\hat{q}_1 \hat{q}_2 b} \hat{p}_1 e^{i\hat{q}_1 \hat{q}_2 b} = \hat{p}_1 + b\hat{q}_2,$$
$$e^{-i\hat{q}^2 g} \hat{p} e^{i\hat{q}^2 g} = \hat{p} + 2g\hat{q}, \quad (C6)$$

from which it is easy to derive that the operator $O(\hat{q})$ leads to

$$\hat{p}_1 \rightarrow \hat{p}_1 + 2b_1 \hat{q}_1 + b_3 \hat{q}_2,$$
$$\hat{p}_2 \rightarrow \hat{p}_2 + 2b_2 \hat{q}_2 + b_3 \hat{q}_1. \quad (C7)$$

This corresponds to the action

$$\begin{pmatrix} \vec{q}' \\ \vec{p}' \end{pmatrix} = \begin{pmatrix} I_2 & 0 \\ M_R & I_2 \end{pmatrix} \begin{pmatrix} \vec{q}' \\ \vec{p}' \end{pmatrix}, \quad (C8)$$

with

$$M_R = \begin{pmatrix} 2b_1 & b_3 \\ b_3 & 2b_2 \end{pmatrix}. \quad (C9)$$

We have hence the identification $b_1 = \sqrt{R}/2$, $b_2 = -\sqrt{R}/2$, $b_3 = \sqrt{1-R}$. Hence we finally obtain the decomposition for the beam splitter Eq. (50).

3. Decomposition of the rotation (exact)

For completeness, even though we do not use its expression, we also provide a decomposition of the rotation gate. Due to the identity

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ s_3 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$
$$\times \begin{pmatrix} 1 & 0 \\ s_2 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ s_1 & 1 \end{pmatrix}, \quad (C10)$$

with $s_1 = \sec\theta + \tan\theta$, $s_2 = \cos\theta$, $s_3 = \cos\theta + (1 + \sin\theta)\tan\theta$, using Eq. (C1) we conclude that

$$e^{i\frac{\theta}{2}(\hat{q}^2+\hat{p}^2)} = \hat{F} e^{\frac{is_3 \hat{q}^2}{2}} \hat{F} e^{\frac{is_2 \hat{q}^2}{2}} \hat{F} e^{\frac{is_1 \hat{q}^2}{2}}. \quad (C11)$$

[1] J. Yoshikawa, S. Yokoyama, T. Kaji, C. Sornphiphatphong, Y. Shiozawa, K. Makino, and A. Furusawa, APL Photon. **1**, 060801 (2016).

[2] C. M. Wilson, G. Johansson, A. Pourkabirian, M. Simoen, J. R. Johansson, F. Nori, and P. Delsing, Nature (London) **479**, 376 (2011).

[3] X. Gu, A. Kockum, A. Miranowicz, Y. Liu, and F. Nori, Phys. Rep. **718–719**, 1 (2017).

[4] M. Aspelmeyer, T. J. Kippenberg, and F. Marquardt, Rev. Mod. Phys. **86**, 1391 (2014).

[5] O. Houhou, H. Aissaoui, and A. Ferraro, Phys. Rev. A **92**, 063843 (2015).

[6] J. Niset, J. Fiurášek, and N. J. Cerf, Phys. Rev. Lett. **102**, 120501 (2009).

[7] R. Namiki, O. Gittsovich, S. Guha, and N. Lütkenhaus, Phys. Rev. A **90**, 062316 (2014).

[8] I. L. Chuang, D. W. Leung, and Y. Yamamoto, Phys. Rev. A **56**, 1114 (1997).

[9] W. Wasilewski and K. Banaszek, Phys. Rev. A **75**, 042316 (2007).

[10] T. C. Ralph, A. J. F. Hayes, and A. Gilchrist, Phys. Rev. Lett. **95**, 100501 (2005).

[11] M. Bergmann and P. van Loock, Phys. Rev. A **94**, 012311 (2016).

[12] M. H. Michael, M. Silveri, R. T. Brierley, V. V. Albert, J. Salmilehto, L. Jiang, and S. M. Girvin, Phys. Rev. X **6**, 031006 (2016).

[13] Z. Leghtas, G. Kirchmair, B. Vlastakis, R. J. Schoelkopf, M. H. Devoret, and M. Mirrahimi, Phys. Rev. Lett. **111**, 120501 (2013).

[14] M. Mirrahimi, Z. Leghtas, V. V. Albert, S. Touzard, R. J. Schoelkopf, L. Jiang, and M. H. Devoret, New J. Phys. **16**, 045014 (2014).

[15] L. Li, C.-L. Zou, V. V. Albert, S. Muralidharan, S. M. Girvin, and L. Jiang, Phys. Rev. Lett. **119**, 030502 (2017).

[16] M. Bergmann and P. van Loock, Phys. Rev. A **94**, 042332 (2016).

[17] D. Gottesman, A. Kitaev, and J. Preskill, Phys. Rev. A **64**, 012310 (2001).

[18] N. C. Menicucci, Phys. Rev. Lett. **112**, 120504 (2014).

[19] T. Douce, D. Markham, E. Kashefi, E. Diamanti, T. Coudreau, P. Milman, P. van Loock, and G. Ferrini, Phys. Rev. Lett. **118**, 070503 (2017).

[20] C. Flühmann, V. Negnevitsky, M. Marinelli, and J. P. Home, Phys. Rev. X **8**, 021001 (2018).

[21] E. Knill, R. Laflamme, and G. J. Milburn, Nature (London) **409**, 46 (2001).

[22] S. Lloyd and S. L. Braunstein, Phys. Rev. Lett. **82**, 1784 (1999).

[23] H. M. Vasconcelos, L. Sanz, and S. Glancy, Opt. Lett. **35**, 3261 (2010).

[24] M. G. A. Paris, M. Cola, and R. Bonifacio, Phys. Rev. A **67**, 042104 (2003).

[25] For bounded quantum polynomial time, the class corresponding to the problems we believe could be efficiently solved by a quantum computer.

[26] A. Bouland, B. Fefferman, C. Nirkhe, and U. Vazirani, arXiv:1803.04402.

[27] D. Vitali, P. Tombesi, and P. Grangier, Appl. Phys. B **64**, 249 (1997).

[28] S. Sefi and P. van Loock, Phys. Rev. Lett. **107**, 170501 (2011).

[29] M. Suzuki, Phys. Lett. A **146**, 319 (1990).

[30] H. Yoshida, Phys. Lett. A **150**, 262 (1990).

[31] Equation (5) of Ref. [28] is derived with different conventions for the commutator $[\hat{q}, \hat{p}]$ from ours. Therefore, the numerical prefactor should change. However, due to a missing factor 4 in the numerator of the lhs in Eq. (5) of Ref. [28], that equation is correct within our notations and we can use it as it is.

[32] K. Fukui, A. Tomita, A. Okamoto, and K. Fujii, Phys. Rev. X **8**, 021054 (2018).

[33] K. Fukui, A. Tomita, and A. Okamoto, Phys. Rev. A **98**, 022326 (2018).

[34] S. Aaronson and A. Arkhipov, Theory Comput. **9**, 143 (2013).

[35] E. Farhi and A. W. Harrow, arXiv:1602.07674.

[36] T. Morimae, K. Fujii, and J. F. Fitzsimons, Phys. Rev. Lett. **112**, 130502 (2014).

[37] S. Aaronson, PostBQP postscripts: A confession of mathematical errors, www.scottaaronson.com/blog/?p=2072.

[38] J. Roslund, R. Medeiros de Araújo, S. Jiang, C. Fabre, and N. Treps, Nat. Photon. **8**, 109 (2014).

[39] R. Medeiros de Araújo, J. Roslund, Y. Cai, G. Ferrini, C. Fabre, and N. Treps, Phys. Rev. A **89**, 053828 (2014).

[40] M. Chen, N. C. Menicucci, and O. Pfister, Phys. Rev. Lett. **112**, 120505 (2014).

[41] S. Yokoyama, R. Ukai, S. C. Armstrong, C. Sornphiphatphong, T. Kaji, S. Suzuki, J.-i. Yoshikawa, H. Yonezawa, N. C. Menicucci, and A. Furusawa, Nat. Photon. **7**, 982 (2013).

[42] X. Su, Y. Zhao, S. Hao, X. Jia, C. Xie, and K. Peng, Opt. Lett. **37**, 5178 (2012).

[43] Y.-S. Ra, C. Jacquard, A. Dufour, C. Fabre, and N. Treps, Phys. Rev. X **7**, 031012 (2017).

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

[45] K. Miyata, H. Ogawa, P. Marek, R. Filip, H. Yonezawa, J.-i. Yoshikawa, and A. Furusawa, Phys. Rev. A **93**, 022301 (2016).

[46] S. Ghose and B. C. Sanders, J. Mod. Opt. **54**, 855 (2007).

[47] B. H. Schneider, A. Bengtsson, I.-M. Svensson, T. Aref, G. Johansson, J. Bylander, and P. Delsing, arXiv:1802.05529.

[48] M. Hofheinz, H. Wang, M. Ansmann, R. C. Bialczak, E. Lucero, M. Neeley, A. D. O'Connell, D. Sank, J. Wenner, J. M. Martinis *et al.*, Nature (London) **459**, 546 (2009).

[49] M. Brunelli, O. Houhou, D. W. Moore, A. Nunnenkamp, M. Paternostro, and A. Ferraro, Phys. Rev. A **98**, 063801 (2018).

[50] K. Fujii and S. Tamate, Sci. Rep. **6**, 25598 (2016).

[51] S. Sefi, V. Vaibhav, and P. van Loock, Phys. Rev. A **88**, 012303 (2013).

[52] F. Arzani, N. Treps, and G. Ferrini, Phys. Rev. A **95**, 052352 (2017).

[53] M. Gu, C. Weedbrook, N. C. Menicucci, T. C. Ralph, and P. van Loock, Phys. Rev. A **79**, 062318 (2009).

[54] R. Ukai, J.-i. Yoshikawa, N. Iwata, P. van Loock, and A. Furusawa, Phys. Rev. A **81**, 032315 (2010).