Anonymous broadcasting of classical information with a continuous-variable topological quantum code

Nicolas C. Menicucci,[1,2] Ben Q. Baragiola,[3,1] Tommaso F. Demarie,[4,5,3] and Gavin K. Brennen[3]

[1]*Centre for Quantum Computation and Communication Technology, School of Science, RMIT University, Melbourne, Victoria 3001, Australia*

[2]*School of Physics, The University of Sydney, Sydney, New South Wales 2006, Australia*

[3]*Centre for Engineered Quantum Systems, Department of Physics and Astronomy, Macquarie University, North Ryde, New South Wales 2109, Australia*

[4]*Singapore University of Technology and Design, 8 Somapah Road, Singapore 487372*

[5]*Centre for Quantum Technologies, National University of Singapore, Block S15, 3 Science Drive 2, Singapore 117542*

(Received 20 April 2015; published 30 March 2018)

Broadcasting information anonymously becomes more difficult as surveillance technology improves, but remarkably, quantum protocols exist that enable provably traceless broadcasting. The difficulty is making scalable entangled resource states that are robust to errors. We propose an anonymous broadcasting protocol that uses a continuous-variable surface-code state that can be produced using current technology. High squeezing enables large transmission bandwidth and strong anonymity, and the topological nature of the state enables local error mitigation.

DOI: 10.1103/PhysRevA.97.032345

I. INTRODUCTION

Almost every aspect of modern society relies on information processing. As digital surveillance capabilities continue to expand, so does demand for guaranteed-anonymous communication strategies. An important primitive for privacy-preserving routines is anonymous broadcasting [1], which can facilitate, for example, tipping off the police anonymously, secret balloting, secure electronic auctions [2], and anonymous cryptocurrency transactions [3]. In the original classical formulation [4] and its improvements [5,6], n players establish shared keys enabling one party to reveal a single bit of information while keeping her identity secret. The first *quantum* protocol allowing one to communicate classical information anonymously was proposed in Ref. [7]. A more efficient and secure quantum protocol for anonymous quantum and classical broadcasting was reported by Christandl and Wehner in Ref. [8]. Here, a trusted resource distributes ahead of time an n-partite entangled state

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}(|0_1 \ldots 0_n\rangle + |1_1 \ldots 1_n\rangle), \tag{1}$$

one qubit to each party. The key feature of this quantum protocol is that it is completely *traceless*—i.e., the sender's identity cannot be determined (better than guessing) even if all resources are made public at the end of the protocol. Remarkably, tracelessness cannot be achieved classically. This protocol and its later improvements [9,10], however, suffer from decoherence from unwanted interactions with the environment. Indeed, the issue of decoherence is rather challenging to overcome, and it has surprisingly been ignored in all previous works.

A solution to this problem is to encode the shared resource in a quantum error-correcting code [11]. A practical code should be fast to prepare and easy to correct using mostly local operations by the players involved. Surface codes [12] satisfy these requirements. These have been extensively studied for the purpose of providing sustained quantum memories or for fault-tolerant quantum computation [13], and recent experiments [14] have built small prototype qubit toric codes. However, the overhead in gates and qubits for such quantum processing is daunting [15].

Here we show that much simpler tasks for communicating *classical information* benefit from the topological protection of such codes. In particular, we present a protocol for quantum-assisted anonymous broadcasting using a recently developed continuous-variable (CV) toric code [16]. The motivation for using this resource is threefold: (1) the topological nature of the state allows for error mitigation; (2) the state can be easily prepared and distributed to the players using Gaussian resources and operations; and (3) using a CV resource allows for a larger communication bandwidth than either the classical or the discrete quantum counterpart. This bandwidth is limited only by the initial squeezing level in the resource.

II. ANONYMOUS BROADCASTING WITH THE QUBIT TORIC CODE

We illustrate the main idea with a qubit toric code. Consider an $n \times m$ square lattice with a sets of vertices $\mathcal{V} = \{v\}$, faces $\mathcal{F} = \{f\}$, and edges $\mathcal{E} = \{e\}$. The lattice lies on a torus, and there is one qubit logically assigned to each edge. The code states are $+1$ eigenstates of the stabilizers [12,17]

$$\hat{A}_v := \prod_{e \in +_v} \hat{X}_e \qquad \forall v \in \mathcal{V}, \tag{2}$$

$$\hat{B}_f := \prod_{e \in \square_f} \hat{Z}_e \qquad \forall f \in \mathcal{F}. \tag{3}$$

On the torus, these operators stabilize a four-dimensional subspace, which encodes two logical qubits [18]. For one of these qubits, the logical $\hat{Z}$ and $\hat{X}$ Pauli operators are,

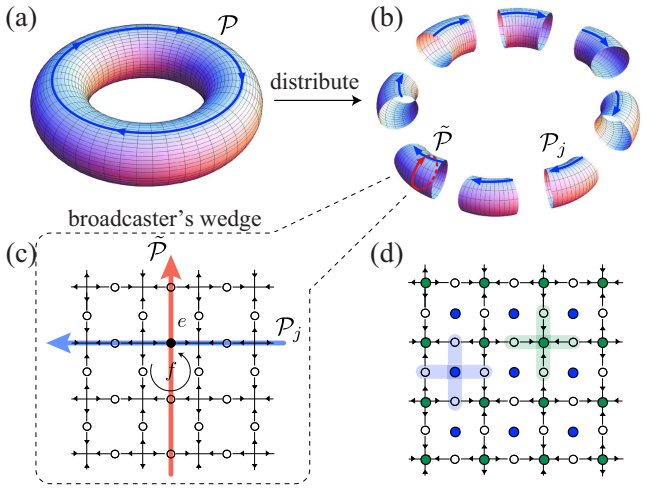

FIG. 1. Sketch of the protocol. (a) A CV surface-code ground state (with squeezed logical modes) is prepared on a torus. The players decide beforehand to perform measurements along a loop around the torus (shown in blue). (b) The state is distributed to the players, one wedge to each. (c) Closeup of the lattice on the broadcaster's wedge. Physical bosonic modes are assigned to each edge, and each edge is assigned an orientation. Similarly, the faces are given a uniform orientation (one face is shown for reference). For the indicated edge e, $f(e,\mathcal{P}) = +1$ with respect to path $\mathcal{P}$ and $f(e,\tilde{\mathcal{P}}) = +1$ with respect to path $\tilde{\mathcal{P}}$ (see Sec. III A). The broadcaster performs the unitary displacement, Eq. (17), on a loop $\tilde{\mathcal{P}}$ around her wedge (shown in red), which encodes a message $r \in \mathbb{R}$. Next, each party j measures an operator, Eq. (18), along an arc $\mathcal{P}_j$ of the loop $\mathcal{P}$ (shown in blue). The players publicly announce their measurement outcomes $\{m_j\}_{j=1}^n$, and the broadcast message is computed as their (noisy) weighted sum. (d) Error mitigation strategy. Additional blue (green) ancillae are quasilocally coupled to modes surrounding faces (vertices), which perform error mitigation by dissipative cooling (see Sec. VII).

respectively, the string operators

$$\hat{Z}_{\mathcal{P}} = \prod_{e\in\mathcal{P}} \hat{Z}_e \quad \text{and} \quad \hat{X}_{\tilde{\mathcal{P}}} = \prod_{e\in\tilde{\mathcal{P}}} \hat{X}_e, \tag{4}$$

where $\mathcal{P}$ is any closed loop along the primal lattice encircling the hole of the torus, and $\tilde{\mathcal{P}}$ is any closed loop along the dual lattice threading through the hole (see Fig. 1).[1]

Here and in the following, we always consider a scenario with n participants, of whom exactly one of them, Alice, wants to anonymously broadcast a public message. The broadcast resource is a toric-code state. In particular, we want a multiqubit state that is simultaneously stabilized by $\hat{A}_v$ $\forall v \in \mathcal{V}$ and also stabilized by $\hat{Z}_{\mathcal{P}}$. One choice for this is

$$|\mathrm{GS}_{00}\rangle := \prod_v \frac{1}{\sqrt{2}}(\hat{I} + \hat{A}_v)|0\ldots0\rangle. \tag{5}$$

The notation "GS" stands for a *ground state* of the toric-code Hamiltonian [12], and this means that $\hat{A}_v$ and $\hat{B}_f$ stabilize the state $\forall v \in \mathcal{V}$ and $\forall f \in \mathcal{F}$. The subscript "00" indicates that both logical qubits are prepared in the logical $|0\rangle$ state. The qubits are logically grouped into n wedges, and the wedges are distributed, one to each player (see Fig. 1).

When Alice wants to anonymously broadcast the message $r = 1$, she performs the string operation $\hat{X}_{\tilde{\mathcal{P}}}$ around the loop on her wedge [see Fig. 1(c)], while for the message $r = 0$, she does nothing. Next, each party j measures qubits in the local $\hat{Z}$ basis along an arc of the wedge and publicly announces the parity $m_j \in \{0,1\}$ of the outcomes. The broadcast message is recovered from the sum $\sum_{j=1}^n m_j = r \pmod 2$.

When using a graph with $|\tilde{\mathcal{P}}| = 1$ (i.e., just one qubit wide, a loop along $\mathcal{P}$), then $|\mathrm{GS}_{00}\rangle$ is just a GHZ state in the $|\pm\rangle$ basis. For such a torus (loop), vertex stabilizers reduce to pairs of adjacent Paulis $(\hat{X}\otimes\hat{X})$ along $\tilde{\mathcal{P}}$, and face stabilizers do not exist. In either case (GHZ or full toric code), the variance of any individual party's measurement is maximal, and no collusion by any proper subset of the nonbroadcasting players will reveal any information about the identity of the broadcaster.

Using a qudit toric code [19] (or qudit GHZ state), the protocol generalizes to allow a single party to anonymously broadcast any d-ary integer $r \in \mathbb{Z}_d$ by applying the string operator $\hat{X}_{\tilde{\mathcal{P}}}^r$, where $\hat{X}$ represents the Weyl-Heisenberg shift operator $\pmod d$. Then, $\sum_{j=1}^n m_j = r \pmod d$. This amounts to broadcasting $\log_2 d$ bits of data per round. Alternatively, such a protocol could instead allow up to $d-1$ broadcasters (out of the n total players) to signal "yes" by each applying $X_{\tilde{\mathcal{P}}}$ around their own wedge. In that case, $\sum_{j=1}^n m_j$ would return the number of "yes" broadcasters $\pmod d$.

The advantage of using a toric-code state instead of a simple GHZ state appears when one considers noise (errors) in the protocol. Notably, since errors in the surface code can be diagnosed by measuring stabilizers, almost all such measurements and corrections are local to each party [see Fig. 1(d)] and can be corrected without disrupting the protocol [20,21]. The exceptions are those stabilizers that straddle the boundary between wedges, and these may be measured with the assistance of Bell pairs shared between nearest-neighbor players to enable nonlocal gates [22]. To do this, the number of entangled pairs needed grows as the number of players and as the width of each wedge. This width, as shown in Appendix B, is a small constant.

III. ANONYMOUS BROADCASTING WITH A CONTINUOUS-VARIABLE TORIC CODE

A. Finitely squeezed continuous-variable surface codes

The ideal CV surface code [23] is a straightforward generalization of the qudit surface code, but it represents an unphysical model because the required states are infinitely squeezed. A finitely squeezed CV surface code is an experimentally accessible, physical approximation of this code [16]. This model starts with an $n \times m$ square lattice with a sets of vertices $\mathcal{V} = \{v\}$, oriented faces $\mathcal{F} = \{f\}$, and oriented edges $\mathcal{E} = \{e\}$ just like in the qudit case [16,19]. An independent, local bosonic mode is logically assigned to each edge of the lattice, for a total of $2nm$ modes, with quadrature operators $\hat{q}_e, \hat{p}_e$ obeying $[\hat{q}_e, \hat{p}_{e'}] = i\delta_{e,e'}$ $(\hbar = 1)$.

[1]There is a second set of similarly defined string operators that serve as logical Pauli operators for the second logical qubit [12]. We only need one logical qubit for the protocol, so we omit their specification to simplify the notation.

A finitely squeezed CV surface code is the null space of a set of nullifiers, $\{\hat{\eta}_i\}$, defined on each vertex and face of the lattice (i.e., $\forall i \in \mathcal{V} \cup \mathcal{F}$). For a given local, modewise squeezing factor s, a finitely squeezed CV surface code is not unique; see Appendix A. We choose to describe relevant features of a CV surface code using the symmetric nullifiers because they are conceptually simpler. These nullifiers are

$$\hat{\eta}_v := \frac{1}{\sqrt{8}} \sum_{e \in +_v} (s\hat{q}_e + is^{-1}\hat{p}_e) \qquad \forall v \in \mathcal{V}, \tag{6a}$$

$$\hat{\eta}_f := \frac{1}{\sqrt{8}} \sum_{e \in \square_f} o(e,f)(s\hat{p}_e - is^{-1}\hat{q}_e) \qquad \forall f \in \mathcal{F}, \tag{6b}$$

where the orientation sign factor $o(e,f) = \pm 1$ if edge e is oriented the same (opposite) as face f. The nullifiers satisfy the commutation relations

$$[\hat{\eta}_v, \hat{\eta}_{v'}] = [\hat{\eta}_f, \hat{\eta}_{f'}] = [\hat{\eta}_v, \hat{\eta}_f] = [\hat{\eta}_v, \hat{\eta}_f^\dagger] = 0 \tag{7}$$

$\forall v \in \mathcal{V}$ and $\forall f \in \mathcal{F}$. As a consequence of finite squeezing, the nullifiers are not Hermitian (whereas they are so in the infinitely squeezed case [23]). This makes them fail to commute with their conjugates when the two share an edge:

$$[\hat{\eta}_v, \hat{\eta}_{v'}^\dagger] \neq 0 \qquad \forall (v,v') \in \mathcal{E}, \tag{8a}$$

$$[\hat{\eta}_f, \hat{\eta}_{f'}^\dagger] \neq 0 \qquad \forall (f \cap f') \in \mathcal{E}. \tag{8b}$$

By definition, a CV surface-code state $|\mathrm{GS}\rangle$ is any state that satisfies

$$\hat{\eta}_v |\mathrm{GS}\rangle = \hat{\eta}_f |\mathrm{GS}\rangle = 0 \qquad \forall v \in \mathcal{V}, \forall f \in \mathcal{F}. \tag{9}$$

Note that we have again used the notation "GS" to indicate that any such state is a *ground state* of a CV surface-code Hamiltonian [16].

It will turn out that the (related, but inequivalent) CV surface-code state that results from measuring a CV cluster state [16] will be easier to work with for our explicit calculations. The differences between this and a symmetric CV surface-code state, along with all explicit details of the construction of the required states and their measurement statistics used for this work, is given in Appendix A.

On the torus there are only $nm - 1$ independent vertex nullifiers and $nm - 1$ independent face nullifiers. Hence, the nullifiers do not span the space of physical modes. And analogous to the two logical qubits encoded in the qubit toric code [13], there are two unconstrained, topological, harmonic-oscillator modes in the CV toric code. These two *logical modes*, which define a two-mode Hilbert space $\mathcal{H}_\mathcal{L}$, are entirely nonlocal and are independent of the squeezing. Since the nullifiers span a $(2nm-2)$-mode Hilbert space $\mathcal{H}_{\mathrm{null}}$, the logical modes and the nullifiers together span the full Hilbert space of the $2nm$ local modes.

The projector onto the toric-code logical subspace is

$$\hat{\mathbf{P}}_\mathcal{L} := |\boldsymbol{\eta}\rangle\langle\boldsymbol{\eta}|_{\mathrm{null}} \otimes \hat{\mathbf{I}}_\mathcal{L}, \tag{10}$$

where the tensor-product decomposition is $\mathcal{H}_{\mathrm{null}} \otimes \mathcal{H}_\mathcal{L}$, and where $|\boldsymbol{\eta}\rangle$ is the simultaneous zero eigenstate of all the nullifiers. We define the two-mode *logical vacuum state* $(|0\rangle \otimes |0\rangle)_\mathcal{L}$ as the restriction of the vacuum state of all local modes to the two-mode logical Hilbert space:

$$(|0\rangle\langle 0| \otimes |0\rangle\langle 0|)_\mathcal{L} := \mathrm{tr}_{\mathrm{null}}[|0\rangle\langle 0|^{\otimes(2nm)}]. \tag{11}$$

This state is pure because we define the mode transformation from local modes to $\mathcal{H}_{\mathrm{null}} \otimes \mathcal{H}_\mathcal{L}$ to be passive (total number conserving). A full description of a finitely squeezed CV toric code goes beyond the scope of this work and will be presented elsewhere.

In the mean time, there are two important states we must identify for our work. We include these below, with their derivation given in Appendix A 2. The first is the *toric-code logical vacuum state*

$$|\mathrm{GS}_{\mathrm{vac}}\rangle := |\boldsymbol{\eta}\rangle_{\mathrm{null}} \otimes (|0\rangle \otimes |0\rangle)_\mathcal{L}, \tag{12}$$

which will be used to demonstrate a proof-of-principle error mitigation strategy in Sec. VII. The second is the state that results from preparing a CV toric-code state by measuring a CV cluster state [16]. This state, which we call the *toric-code logical squeezed state*, will be used to analyze the anonymous broadcasting protocol below. It has the form

$$|\mathrm{GS}_{\mathrm{sq}}\rangle := |\tilde{\boldsymbol{\eta}}\rangle_{\mathrm{null}} \otimes (|0;s\rangle \otimes |0;s\rangle)_\mathcal{L}, \tag{13}$$

where $|0;s\rangle$ is a momentum-squeezed vacuum state with squeezing factor s. Nevertheless, it is still a ground state (hence, "GS") of a CV toric-code Hamiltonian [16]. The nullifiers used to define $|\mathrm{GS}_{\mathrm{sq}}\rangle$ are slightly different from the symmetric nullifiers shown in Eqs. (6)—hence the tilde on $\tilde{\boldsymbol{\eta}}$. The logical subspace, however, is exactly the same in both cases. (For further information, see Appendix A).

The reasons we use this state, despite the aforementioned complications, are (1) we know how to make it from a large-scale CV cluster state [16], (2) large-scale CV cluster states have been demonstrated experimentally (see Sec. VIII), and (3) the covariance matrix for this state has a pp submatrix that is of a particularly simple form, which simplifies the analysis of its performance for anonymous broadcasting (see Appendix A).

For completeness, we note that in standard quantum-optics language [24],

$$|0;s\rangle := \hat{S}(-\ln s)|0\rangle, \ \hat{S}(\xi) := \exp\left[\tfrac{1}{2}(\xi^* \hat{a}^2 - \xi \hat{a}^{\dagger 2})\right], \tag{14}$$

where $\xi = -\ln s$ is the squeezing parameter. Thus, with our conventions, we have for any single mode

$$\langle 0;s|\hat{q}^2|0;s\rangle = \frac{s^2}{2}, \quad \langle 0;s|\hat{p}^2|0;s\rangle = \frac{1}{2s^2}. \tag{15}$$

The case $s = 1$ corresponds to the ordinary vacuum state.

B. Anonymous broadcasting protocol

Given a CV toric code, the anonymous-broadcasting protocol is summarized in protocol I and graphically represented in Fig. 1. We make use of a nonlocal string momentum operator

$$\hat{M} := \frac{1}{\sqrt{|\mathcal{P}|}} \sum_{e \in \mathcal{P}} f(e,\mathcal{P})\hat{p}_e. \tag{16}$$

where $\mathcal{P}$ is a loop around on the primal lattice. For each edge, the orientation factor $f(e,\mathcal{P}) = \pm 1$ if the edge has the same (opposite) orientation as the path $\mathcal{P}$. For the toric-code logical squeezed state $|\mathrm{GS}_{\mathrm{sq}}\rangle$, the variance of the string momentum operator $\hat{M}$ is $(\Delta M)^2 = \frac{1}{2s^2}$, with $\langle \hat{M} \rangle = 0$, as shown in

Protocol 1 Finite-squeezing CV anonymous broadcasting.

Steps of the protocol

1. **Initialization:** A CV toric-code logical squeezed state $|\mathrm{GS}_{\mathrm{sq}}\rangle$ is prepared [Eq. (13)]. The state is distributed, one wedge to each player.
2. **Broadcasting:** To anonymously broadcast the real number r, Alice performs the displacement $\hat{D}_r$ [Eq. (17)] on her wedge.
3. **Local measurements:** Each player measures her portion of the string momentum, $\hat{M}_j$ [Eq. (18)], and records the outcome $m_j \in \mathbb{R}$.
4. **Determining the broadcast message:** All players publicly announce their results $\{m_j\}$. The message broadcast by Alice can be inferred from the noisy weighted sum M in Eq. (19).

Appendix A. The torus is divided into n wedges, and each is distributed to a single player. To broadcast the real number r, Alice wishes to perform a displacement of the string momentum $\hat{M} \mapsto \hat{M} + r$ by means that are not detectable once the measurements have begun [8]. To this end, she applies a displacement on the dual lattice along the loop $\tilde{\mathcal{P}}$ by applying the unitary

$$\hat{D}_r = \exp\left(ir\sqrt{|\tilde{\mathcal{P}}|} \sum_{e\in\tilde{\mathcal{P}}} f(e,\tilde{\mathcal{P}})\hat{q}_e \right) \tag{17}$$

on her wedge. Here, $f(e,\tilde{\mathcal{P}}) = \pm 1$ if the edge e has the same (opposite) direction as the framing of the path $\tilde{\mathcal{P}}$, where the framing of a path is to the right and normal to its direction [see Fig. 1(b)].

After the broadcasting stage of the protocol, the string momentum operator $\hat{M}$ is measured, with each player contributing a measurement on her wedge. The party holding wedge $j \in \{1,2,\ldots,n\}$ measures her portion of the string momentum operator,

$$\hat{M}_j := \frac{1}{\sqrt{|\mathcal{P}_j|}} \sum_{e\in\mathcal{P}_j} o(e)\hat{p}_e, \tag{18}$$

along an arc $\mathcal{P}_j$ of the loop $\mathcal{P}$. Each party records the outcome $m_j \in \mathbb{R}$. During the measurements, the path $\mathcal{P} = \bigcup_{j=1}^{n} \mathcal{P}_j$ must be a closed loop. This implies preagreement between the players and active classical communication during the protocol to establish a different connected path in case of errors at the wedge boundaries.

In the final step of the protocol, all players publicly announce their measurement results $\{m_j\}$. The broadcast message is recovered by calculating the noisy, weighted sum,

$$M = \frac{1}{\sqrt{|\mathcal{P}|}} \sum_{j=1}^{n} \sqrt{|\mathcal{P}_j|}\, m_j, \tag{19}$$

which is a classical random variable with mean r and variance $(\Delta M)^2 = \frac{1}{2s^2}$, as shown in Appendix A.[2]

[2]We have assumed, without loss of generality, that the face and edge orientation at the edge e_A of the intersection of the arc $\mathcal{P}$(Alice) and the loop $\tilde{\mathcal{P}}$ satisfies $(-1)^{f(e_A)+o(e_A)} = 1$; otherwise, r acquires that sign.

IV. BROADCAST CHANNEL CAPACITY

In this section, we calculate the channel capacity for the broadcast protocol discussed above. Since the message space is unbounded, the capacity is technically infinite. Therefore, in order to get a finite quantity, we will calculate the channel capacity conditioned on a fixed variance τ^2 of the message to be broadcast. (This does not specify the shape of the broadcast message distribution, of course, since two possibilities would be a Gaussian with variance τ^2 and a binary distribution with δ-function support only at $\pm\tau$.) The result presented here was first calculated by Shannon [25,26]. We include our own derivation in order to maintain a self-contained presentation and because it is straightforward and rather elegant.

For an input broadcast message $R \in \mathbb{R}$ and some output reconstructed message $M \in \mathbb{R}$, the variance-restricted channel capacity is $C = \max_{p_R(r)} I(R;M)$, where the maximum is over all input probability distributions $p_R(r)$ with variance τ^2, and $I(R;M) = H(M) - H(M|R)$ is the mutual information between R and M [27]. The conditional probability $p_{M|R}(m|r) = N_{m,(\Delta M)^2}(r)$ is a normal distribution [see Eq. (C1)] in output m with mean r and variance $(\Delta M)^2$ from Eq. (A36).

For an arbitrarily distributed R with mean μ and variance τ^2, the cumulant vector [28] for R is $\mathbf{c}_R = (\mu,\tau^2,c_3,c_4,\ldots)$, and that for M is called $\mathbf{c}_M$. Using the law of total probability,

$$\begin{aligned} p_M(m) &= \int dr\; p_{M|R}(m|r)p_R(r) \\ &= (N_{0,(\Delta M)^2} * p_R)(m), \end{aligned} \tag{20}$$

where $*$ indicates convolution. Cumulants add under convolution [28]. Therefore,

$$\begin{aligned} \mathbf{c}_M &= \mathbf{c}_R + (0,(\Delta M)^2,0,\ldots) \\ &= (\mu,\tau^2 + (\Delta M)^2,c_3,c_4,\ldots). \end{aligned} \tag{21}$$

Note that $H(M|R)$ is fixed by the channel since $p_{M|R}(m|r)$ is a function only of $(m-r)$, and thus averaging over R does not change the entropy. Therefore, the only difference that p_R makes to $I(R;M)$ is through $H(M)$. We can maximize $I(R;M)$ by maximizing $H(M)$ (subject to the τ^2 constraint), which means requiring that p_M be Gaussian (see Appendix C) with variance $\tau^2 + (\Delta M)^2$ and arbitrary mean. This can be achieved by requiring all cumulants beyond the second of $\mathbf{c}_M$ to be zero—i.e., $\mathbf{c}_M = (\mu,\tau^2 + (\Delta M)^2,0,0,\ldots)$. Therefore, $\mathbf{c}_R = (\mu,\tau^2,0,0,\ldots)$, which means that the maximizing p_R is also Gaussian. For a given variance τ^2 of the message, this choice maximizes the mutual information and thus defines the (variance-restricted) channel capacity (see Appendix C):

$$\begin{aligned} C &= \tfrac{1}{2}\log[2\pi e(\tau^2 + (\Delta M)^2)] - \tfrac{1}{2}\log[2\pi e(\Delta M)^2] \\ &= \tfrac{1}{2}\log(1+\alpha), \end{aligned} \tag{22}$$

where the signal-to-noise ratio (SNR) of the broadcast is

$$\alpha = \frac{\tau^2}{(\Delta M)^2}, \tag{23}$$

and where the base of the logarithm is left unspecified because it merely determines the units (base 2 for bits, base e for nats, etc.). There exist lattice codes for sending digital information through such a channel that achieve this capacity [29].

V. BROADCASTER ANONYMITY

Because of finite squeezing, the broadcast will not be completely anonymous. We precisely quantify the tradeoff between anonymity and channel capacity in terms of squeezing and hence signal-to-noise ratio (SNR). We first discuss anonymity: This is predicated on the assumed inability to identify the broadcaster based on the local measurement outcomes. The degree to which this is true depends on the SNR of the message strength to the noise in the local measurement. A high degree of anonymity depends on this being small. However, the signal strength cannot be too small lest the broadcast be too weak to be detected.

In this section we quantify the anonymity of the broadcast channel in terms of how much information about the identity of the sender leaks out into the classical measurement record. First, we need the measurement covariance matrix shared among the players prior to the broadcast. This is done for various cases in Appendix A, including the CV toric code as well as simpler graphs such as the CV GHZ state and the open boundary CV surface code. We assume a surface-code state with toroidal boundary conditions, as discussed in Appendix A 5, in order to simplify the calculation by putting all players on the same footing. A similar calculation is possible using other boundary conditions and more general assumptions, but our purpose is simply to quantify the amount of anonymity in a basic instance of the protocol.

A. Players' covariance matrix after broadcast

In Appendix A 5, we calculate the covariance matrix of the players' individual measurement outcomes before any broadcast is made, given by Eqs. (A34)–(A35). The full covariance matrix for the random measurement-results vector $\mathbf{M}$ can be written using the definition for the circulant matrix in Appendix C, Eq. (C7):

$$\mathbf{\Sigma} := \langle \mathbf{M}\mathbf{M}^{\mathrm{T}} \rangle = \frac{-s^2}{2w} \mathbf{C}_n \left(-\frac{w}{s^4} - 2 \right), \tag{24}$$

where w is the width of each wedge.

Let the identity of Alice (the broadcaster) be associated with a random variable $A \in \{1, \ldots, n\}$. (It is random because other people wishing to discover her identity do not know who she is.) We assume that she wishes to broadcast a real number $r \in \mathbb{R}$, which we shall treat as an instantiation of a Gaussian-distributed random variable $R \sim N_{0,\tau^2}(r)$, as is prescribed to be optimal in Sec. IV. Conditioned on Alice actually being player a and applying the string-momentum shift along $\tilde{\mathcal{P}}$ to implement the broadcast, the actual random measurement outcome for each player can be written

$$M_{j|a} := M_j + \sqrt{n} R \delta_{ja}, \tag{25}$$

since $n = |\mathcal{P}|/|\mathcal{P}_j|$. Then, the variance and covariance of the actual measurement outcomes *when averaged over the actual message sent* are, respectively,

$$\langle M_{j|a}^2 \rangle = \frac{1}{2s^2} + \frac{s^2}{w} + n\tau^2 \delta_{ja}, \tag{26}$$

$$\langle M_{j|a} M_{j\pm1|a} \rangle = \frac{-s^2}{2w}. \tag{27}$$

This gives the following covariance matrix of the actual random vector of outcomes, conditioned on the broadcaster being player a:

$$\mathbf{\Sigma}_{|a} := \langle \mathbf{M}_{|a} \mathbf{M}_{|a}^{\mathrm{T}} \rangle = \mathbf{\Sigma} + n\tau^2 \mathbf{e}_{aa}, \tag{28}$$

where $\mathbf{e}_{aa}$ is a matrix with a 1 in the (a,a) entry and zeros everywhere else.

B. Information leakage about broadcaster's identity

We model the leakage of information about the broadcaster's identity in terms of the mutual information $I(\mathbf{M}; A)$ between the random vector of measurement outcomes $\mathbf{M}$ (averaged over the broadcaster A and the message R) and the random variable A identifying the broadcaster [27]. In other words, how much information about A can be extracted from $\mathbf{M}$? More specifically, this measures how much the entropy of A is reduced (on average) if one has access to the measurement record $\mathbf{M}$:

$$I(\mathbf{M}; A) = H(A) - H(A|\mathbf{M}). \tag{29}$$

Symmetry of the mutual information means that we can also write it as

$$I(\mathbf{M}; A) = H(\mathbf{M}) - H(\mathbf{M}|A), \tag{30}$$

which will be more straightforward to calculate.

The conditional entropy is the entropy of $\mathbf{M}$ if one knows who the broadcaster is, averaged over both the message and the broadcaster's identity:

$$H(\mathbf{M}|A) = \langle -\log p_{\mathbf{M}|A}(\mathbf{M}|A) \rangle_{\mathbf{M},A}. \tag{31}$$

We assume, for simplicity, that we have no initial information about the broadcaster's identity—a flat prior over all possible broadcasters:

$$A \sim p_A(a) = \frac{1}{n}. \tag{32}$$

From the subsection above, we know the distribution of the message $\mathbf{M}_{|a}$ conditioned on knowing who the broadcaster is:

$$\mathbf{M}_{|a} \sim p_{\mathbf{M}|A}(\mathbf{m}|a) = N_{\mathbf{0},\mathbf{\Sigma}_{|a}}(\mathbf{m}), \tag{33}$$

where we used the notation for a multivariate Gaussian from Eq. (C2). Therefore (see Appendix C),

$$\begin{aligned} H(\mathbf{M}|A) &= \left\langle \tfrac{1}{2} \log \det(2\pi e \mathbf{\Sigma}_{|A}) \right\rangle_A \\ &= \tfrac{1}{2} \log \det[2\pi e (\mathbf{\Sigma} + n\tau^2 \mathbf{e}_{1,1})]. \end{aligned} \tag{34}$$

Note that $n\tau^2$ could have just as well been added to any other location on the diagonal; the (1,1) entry was chosen by fiat.

Using the law of total probability, we can calculate

$$\begin{aligned} \mathbf{M} \sim p_{\mathbf{M}}(\mathbf{m}) &= \sum_{a=1}^{n} p_{\mathbf{M}|A}(\mathbf{m}|a) p_A(a) \\ &= \frac{1}{n} \sum_{a=1}^{n} N_{\mathbf{0},\mathbf{\Sigma}_{|a}}(\mathbf{m}). \end{aligned} \tag{35}$$

This is not a Gaussian; rather, it is a mixture of Gaussians with different covariance matrices. Nevertheless, we can use

the law of total expectation to calculate the post-measurement covariance matrix

$$\begin{aligned}\langle \mathbf{M}\mathbf{M}^{\mathrm{T}}\rangle_{\mathbf{M}} &= \frac{1}{n}\sum_{a=1}^{n}\langle \mathbf{M}_{|a}\mathbf{M}_{|a}^{\mathrm{T}}\rangle_{\mathbf{M}|a} \\ &= \frac{1}{n}\sum_{a=1}^{n}\boldsymbol{\Sigma}_{|a} \\ &= \boldsymbol{\Sigma}+\tau^2\mathbf{I}. \end{aligned} \tag{36}$$

By Eq. (C5) in Appendix C, we can use this to place an upper bound on $H(\mathbf{M})$:

$$H(\mathbf{M}) \leqslant \tfrac{1}{2}\log\det[2\pi e(\boldsymbol{\Sigma}+\tau^2\mathbf{I})]. \tag{37}$$

And hence, combining Eqs. (34) and (37), we have

$$I(\mathbf{M};A) \leqslant \frac{1}{2}\log\left[\frac{\det(\boldsymbol{\Sigma}+\tau^2\mathbf{I})}{\det(\boldsymbol{\Sigma}+n\tau^2\mathbf{e}_{1,1})}\right]. \tag{38}$$

For convenience, we define

$$\epsilon = \frac{(\Delta M)^2}{(\Delta M_j)^2-(\Delta M)^2}, \tag{39}$$

such that the quantities that appear in Eq. (38) can be written

$$\boldsymbol{\Sigma}+\tau^2\mathbf{I} = \frac{-s^2}{2w}\mathbf{C}_n[-2(1+\epsilon+\epsilon\alpha)], \tag{40}$$

$$\boldsymbol{\Sigma}+n\tau^2\mathbf{e}_{1,1} = \frac{-s^2}{2w}\mathbf{C}_n[-2(1+\epsilon),-2n\epsilon\alpha], \tag{41}$$

where α is the SNR given in Eq. (23). Using Eqs. (C14), and (C17), we obtain an explicit bound on the amount of information about the broadcaster's identity leaked within the measurement outcomes (assuming $n \geqslant 3$):

$$I(\mathbf{M};A) \leqslant \frac{1}{2}\log\left\{\frac{T_n(1+\epsilon+\epsilon\alpha)-1}{\left(1+\epsilon\alpha\frac{\partial}{\partial\epsilon}\right)[T_n(1+\epsilon)-1]}\right\}, \tag{42}$$

where T_n is the nth-order Chebyshev polynomial of the first kind, valid for $n \geqslant 3$. The mathematical form of Eq. (42) can be interpreted as comparing a shift in a function [namely, $f(\epsilon) \mapsto f(\epsilon+\epsilon\alpha)$, where $f(\epsilon) = T_n(1+\epsilon)-1$] to its first-order Taylor-series approximation. When this is a good approximation, anonymity is high, and little identifying information leaks out.

The only reason Eq. (42) is not an equality is that we used the fact that the entropy of a mixture of Gaussians is upper bounded by the entropy of a Gaussian with the same covariance as that of the mixture. When this is a bad approximation, it is possible that the right-hand side of Eq. (42) could exceed $H(A) = \log n$, while the actual value of $I(\mathbf{M};A)$ never will. Also note that $I(\mathbf{M};A)$ as calculated is not additive under multiple repetitions of the protocol with the same broadcaster because after each run, the prior $p_A(a)$ about the sender's identity will have changed based on the new information, requiring a new calculation. Nevertheless, Eq. (42) provides an estimate of the anonymity of the broadcaster in an asymptotic sense to be described shortly. (A calculation of single-shot probability of detection in a special case of the protocol is deferred to Sec. VI.)

Anonymity is high whenever Alice's post-broadcast probability of discovery is very low. Since we have formulated the problem as a classical channel leaking (Shannon) information about Alice's identity, the relevant metric is the asymptotic behavior of the channel under N independent uses for large N, each with a (potentially) different broadcaster each time [27]. Assuming each use is independent and the broadcaster and message are identically distributed each time, the asymptotic equipartition theorem states that the probability of a sequence $(a_1,\ldots,a_N)$ of broadcasters given N independent broadcast events satisfies

$$\Pr(a_1,\ldots,a_N) \approx 2^{-NH(A|\mathbf{M})} \tag{43}$$

with high probability [27]. We can now define

$$p := 2^{-H(A|\mathbf{M})} = \frac{2^{I(\mathbf{M};A)}}{2^{H(A)}} \tag{44}$$

using log base 2. Since $p = \lim_{N\to\infty}[\Pr(a_1,\ldots,a_N)]^{1/N}$ with high probability, we can interpret p as the *geometric-mean probability that the broadcaster is correctly identified* over many independent broadcast events.

Note, however, that in any particular instance of the broadcast, p would not be a valid estimate of the probability that that particular broadcaster is correctly guessed. We press on nonetheless using p because the analytic form of the mutual information makes it convenient for analysis. We perform the single-shot analysis using the (less accessible but more appropriate) min-entropy in Sec. VI.

We want the quantity p to be small ($p \ll 1$). Replacing $I(\mathbf{M};A)$ in Eq. (44) with its upper bound from Eq. (42) and then squaring both sides only strengthens the condition, which lets us write the following in the limit of a good resource state ($\epsilon \ll 1$):

$$n^2 \gg 1+\frac{(n^2-1)\alpha^2\epsilon}{6(1+\alpha)}+O(\epsilon^2). \tag{45}$$

Solving for α and dropping terms of $O(\epsilon^2)$ gives the bound:

$$\alpha\epsilon \ll 6. \tag{46}$$

Since $\alpha\epsilon$ is the SNR of the broadcast message with respect to the excess noise in each of the local measurements, we can summarize this condition by saying that *anonymity is high when the broadcast message is sufficiently obscured by the local measurement noise*.

Clearly, there is a tradeoff between anonymity and channel capacity.[3] In particular, for a fixed value of the squeezing s, high SNR provides a larger channel capacity at the expense of lower anonymity. The opposite is also true: Small SNR corresponds to higher anonymity but smaller channel capacity. We explore this tradeoff in Fig. 2 for a fixed squeezing factor $s = 10$, corresponding to 20 dB.

VI. SINGLE-SHOT PROBABILITY OF DETECTION

Here we consider a different scenario in order to make a more precise calculation of the guarantee of anonymity in

[3]The variance restriction on the capacity is henceforth understood.

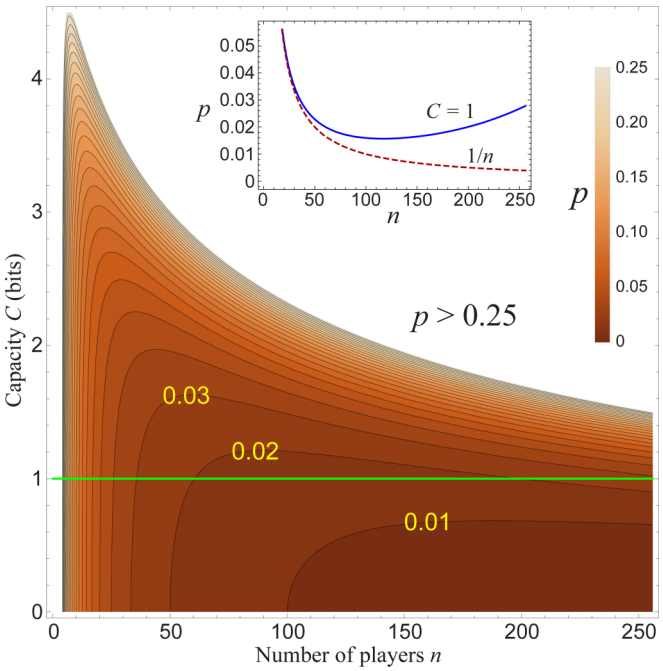

FIG. 2. Contour plot of the geometric-mean probability p that the broadcaster is correctly identified during the protocol as a function of the number of players n and the channel capacity C [Eq. (22)] in the limit of a large number of independent broadcast events. More precisely, we plot an upper bound on p, which we calculate using Eq. (44) and the upper bound for $I(\mathbf{M},A)$ from Eq. (42). Contours corresponding to $p = 0.01, 0.02, 0.03$ are labeled, and subsequent contours increase by 0.01 each. The white region corresponds to $p > 0.25$. The squeezing is 20 dB ($s = 10^{(\#\mathrm{dB})/20} = 10$), and each player's wedge width is $w = 6$ (see Appendix B). The inset shows (i) a solid blue curve corresponding to a cross section of the main plot along the green $C = 1$ line and (ii) a dashed red curve corresponding to $p = 1/n$. The latter corresponds to perfect tracelessness (no more risk than guessing randomly), which is only achieved in the trivial limit of no broadcast ($C = 0$) or, for any $C > 0$, in the asymptotic limit of infinite squeezing.

a single-shot setting. As mentioned above, the min-entropy (rather than the Shannon entropy) is required for this. Furthermore, rather than considering channel capacity, which like the Shannon entropy is another asymptotic concept [27], here we consider a binary broadcast message rather than a real number being broadcast. Thus, our measure of success of the broadcast is in terms of the probability that the message is received as the opposite of what was sent (bit-flip error), and the probability of correct detection is calculated exactly in this single-shot scenario.

As before, player A (the broadcaster) is picked uniformly randomly from all players, but now players agree ahead of time on a simple binary encoding: *Only the sign of the broadcast message matters*. For simplicity, we will restrict to just two possible values of the real-valued broadcast message $R \in \{+r_0, -r_0\}$. The probability that the binary message is received correctly is just the probability that M (the received broadcast message) has the same sign as R (the message being broadcast). For a particular message $r \in \mathbb{R}$, we saw in Sec. III B that $M_{|r} \sim N_{r,(\Delta M)^2}(m)$, where $(\Delta M)^2 = \frac{1}{2s^2}$. By symmetry, for either choice of $r = \pm r_0$, the probability of misidentifying the binary broadcast message is therefore

$$p_{\mathrm{err}} = \int_{-\infty}^{0} dm\, N_{r_0,(2s^2)^{-1}}(m) = \frac{1}{2}\operatorname{erfc}(sr_0), \tag{47}$$

where the complementary error function $\operatorname{erfc} x = 1 - \operatorname{erf} x$. We can rearrange this to obtain the value of r_0 that gives a desired p_{err}:

$$r_0 = \frac{1}{s}\operatorname{erfc}^{-1}(2p_{\mathrm{err}}). \tag{48}$$

Without loss of generality, we can assume that this (positive) value r_0 is the broadcast message since symmetry guarantees that the probability of discovery will not depend on the sign of the broadcast message, only on its magnitude.

We will need the following explicit definitions and probability calculations (see Appendix C for notation):

$$A \sim p_A(a) = \frac{1}{n}, \tag{49}$$

$$\mathbf{M}_{|A} \sim p_{\mathbf{M}|A}(\mathbf{m}|a) = N_{r_0\mathbf{e}_a,\boldsymbol{\Sigma}}(\mathbf{m}), \tag{50}$$

$$(\mathbf{M},A) \sim p_{\mathbf{M},A}(\mathbf{m},a) = \frac{1}{n}N_{r_0\mathbf{e}_a,\boldsymbol{\Sigma}}(\mathbf{m}), \tag{51}$$

$$\mathbf{M} \sim p_{\mathbf{M}}(\mathbf{m}) = \frac{1}{n}\sum_a N_{r_0\mathbf{e}_a,\boldsymbol{\Sigma}}(\mathbf{m}), \tag{52}$$

$$A_{|\mathbf{M}} \sim p_{A|\mathbf{M}}(a|\mathbf{m}) = \frac{N_{r_0\mathbf{e}_a,\boldsymbol{\Sigma}}(\mathbf{m})}{\sum_{a'} N_{r_0\mathbf{e}_{a'},\boldsymbol{\Sigma}}(\mathbf{m})}, \tag{53}$$

where $\mathbf{e}_a$ is a vector of all zeros except for a 1 in slot a. The distributions for A and $\mathbf{M}_{|A}$ are prescribed, from which all of the others can be obtained using the laws of probability.

The min-entropy of a random variable $X \sim p_X(x)$ is

$$H_{\min} := -\log \max_x p_X(x). \tag{54}$$

The min-entropy (with log base 2) is related to the probability of guessing a random variable X [30]. When given *a particular set* of data y, we can immediately write

$$\begin{aligned} p_{\mathrm{g}}(X|Y=y) &:= \Pr(\text{guess } X \text{ correctly}|Y=y) \\ &= 2^{-H_{\min}(X|Y=y)} = \max_x p_{X|Y}(x|y). \end{aligned} \tag{55}$$

To achieve this, one simply guesses that

$$X = \arg\max_x p_{X|Y}(x|y). \tag{56}$$

That is, the best guess for X is the highest-probability outcome x consistent with the data y. Averaging over the data, one obtains the *average* correct guessing probability [30]:

$$\begin{aligned} p_{\mathrm{g}}(X|Y) &= \sum_y p_Y(y) p_{\mathrm{g}}(X|Y=y) \\ &= \sum_y p_Y(y) \max_x p_{X|Y}(x|y). \end{aligned} \tag{57}$$

In our case,

$$\begin{aligned} p_{\mathrm{g}}(A|\mathbf{M}) &= \int d^n m\, p_{\mathbf{M}}(\mathbf{m}) \max_a p_{A|\mathbf{M}}(a|\mathbf{m}) \\ &= \frac{1}{n}\int d^n m \max_a N_{r_0\mathbf{e}_a,\boldsymbol{\Sigma}}(\mathbf{m}). \end{aligned} \tag{58}$$

Simplifying this expression is somewhat involved. We start by noting the identity

$$N_{\mathbf{0},\boldsymbol{\Sigma}}(\mathbf{x}) = |\det \mathbf{L}| N_{\mathbf{0},\mathbf{L}\boldsymbol{\Sigma}\mathbf{L}^{\mathrm{T}}}(\mathbf{L}\mathbf{x}) \tag{59}$$

for any invertible matrix $\mathbf{L} \in \mathbb{R}^{n\times n}$. Thus,

$$\begin{aligned} &p_{\mathrm{g}}(A|\mathbf{M}) \\ &= \frac{1}{n}\int d^n m \ \max_a N_{\mathbf{0},\boldsymbol{\Sigma}}(\mathbf{m} - r_0\mathbf{e}_a) \\ &= \frac{1}{n}\int d^n m \, |\det \boldsymbol{\Sigma}^{-1}| \max_a N_{\mathbf{0},\boldsymbol{\Sigma}^{-1}}(\boldsymbol{\Sigma}^{-1}\mathbf{m} - r_0\boldsymbol{\Sigma}^{-1}\mathbf{e}_a). \end{aligned} \tag{60}$$

Changing variables,

$$\mathbf{u} = \boldsymbol{\Sigma}^{-1}\mathbf{m}, \tag{61}$$

$$d^n u = |\det \boldsymbol{\Sigma}^{-1}| d^n m, \tag{62}$$

we have

$$\begin{aligned} &p_{\mathrm{g}}(A|\mathbf{M}) \\ &= \frac{1}{n}\int d^n u \ \max_a N_{\mathbf{0},\boldsymbol{\Sigma}^{-1}}(\mathbf{u} - r_0\boldsymbol{\Sigma}^{-1}\mathbf{e}_a) \\ &= \frac{(\det 2\pi\boldsymbol{\Sigma}^{-1})^{-1/2}}{n} \\ &\quad \times \int d^n u \ \max_a \exp\left[-\frac{1}{2}(\mathbf{u} - r_0\boldsymbol{\Sigma}^{-1}\mathbf{e}_a)^{\mathrm{T}}\boldsymbol{\Sigma}(\mathbf{u} - r_0\boldsymbol{\Sigma}^{-1}\mathbf{e}_a)\right] \\ &= \frac{(\det 2\pi\boldsymbol{\Sigma}^{-1})^{-1/2}}{n} \\ &\quad \times \int d^n u \ \max_a \exp\left[-\frac{1}{2}\mathbf{u}^{\mathrm{T}}\boldsymbol{\Sigma}\mathbf{u} + r_0\mathbf{u}^{\mathrm{T}}\mathbf{e}_a - \frac{r_0^2}{2}\mathbf{e}_a^{\mathrm{T}}\boldsymbol{\Sigma}^{-1}\mathbf{e}_a\right] \\ &= \frac{c_{\boldsymbol{\Sigma}}}{n}\int d^n u \ N_{\mathbf{0},\boldsymbol{\Sigma}^{-1}}(\mathbf{u}) \max_a \exp(r_0 u_a) \\ &= \frac{c_{\boldsymbol{\Sigma}}}{n}\int d^n u \ N_{\mathbf{0},\boldsymbol{\Sigma}^{-1}}(\mathbf{u}) \exp\left(r_0 \max_a u_a\right), \end{aligned} \tag{63}$$

where we have defined

$$c_{\boldsymbol{\Sigma}} := \exp\left(-\frac{r_0^2}{2}\mathbf{e}_a^{\mathrm{T}}\boldsymbol{\Sigma}^{-1}\mathbf{e}_a\right) = \exp\left(-\frac{r_0^2}{2n}\operatorname{tr}\boldsymbol{\Sigma}^{-1}\right) \tag{64}$$

by the fact that $\boldsymbol{\Sigma}$ is invariant under permutation of the players' labels ($a \to a+1$).

Now we employ a trick: We carve up $\mathbb{R}^n$ into n cones $\{K_j\}_{j=1}^n$, defined by

$$K_j := \{\mathbf{u} \in \mathbb{R}^n \mid u_k \leqslant u_j \ \forall k \neq j\}. \tag{65}$$

Intuitively, this is easy to understand: Every point $\mathbf{u} \in \mathbb{R}^n$ is an n-tuple of real numbers. The index j of the maximum entry of this n-tuple tells you which cone K_j the point belongs to. (In the case where there is more than one maximum entry, just choose the one with smallest index.) In this way, we can *uniquely* partition $\mathbb{R}^n$ into these n cones—i.e., $\mathbb{R}^n = \bigcup_{j=1}^n K_j$ (with any overlap of the cones being of measure 0). Thus, we can write

$$\begin{aligned} p_{\mathrm{g}}(A|\mathbf{M}) &= \frac{c_{\boldsymbol{\Sigma}}}{n}\sum_{j=1}^n \int_{K_j} d^n u \ N_{\mathbf{0},\boldsymbol{\Sigma}^{-1}}(\mathbf{u}) \exp\left(r_0 \max_a u_a\right) \\ &= \frac{c_{\boldsymbol{\Sigma}}}{n}\sum_{j=1}^n \int_{K_j} d^n u \ N_{\mathbf{0},\boldsymbol{\Sigma}^{-1}}(\mathbf{u}) \exp(r_0 u_j) \\ &= c_{\boldsymbol{\Sigma}} \int_{K_1} d^n u \ N_{\mathbf{0},\boldsymbol{\Sigma}^{-1}}(\mathbf{u}) \exp(r_0 u_1), \end{aligned} \tag{66}$$

where we used the fact that the value of the integral is the same for each cone K_j. Notice that we never need to explicitly calculate $\boldsymbol{\Sigma}^{-1}$. The final Gaussian has $\boldsymbol{\Sigma}$ in the actual exponential, and $\frac{1}{n}\operatorname{tr}\boldsymbol{\Sigma}^{-1}$ (found within $c_{\boldsymbol{\Sigma}}$) is just the harmonic mean of the eigenvalues of $\boldsymbol{\Sigma}$.

We succeeded in partially analytically evaluating this integral, obtaining an expression that can be written solely in terms of the cumulative distribution function (CDF) of a multivariate Gaussian. Unfortunately, it appears that there is no known analytic form for the CDF of a high-dimensional multivariate Gaussian. While various numerical techniques and approximations exist [31], we found it sufficient for small n to have MATHEMATICA evaluate the integral as in Eq. (66). The results are shown in Fig. 3 for $p_{\mathrm{err}} = 1\%$ and $p_{\mathrm{err}} = 0.0001\%$ with several values of n and various levels of squeezing.

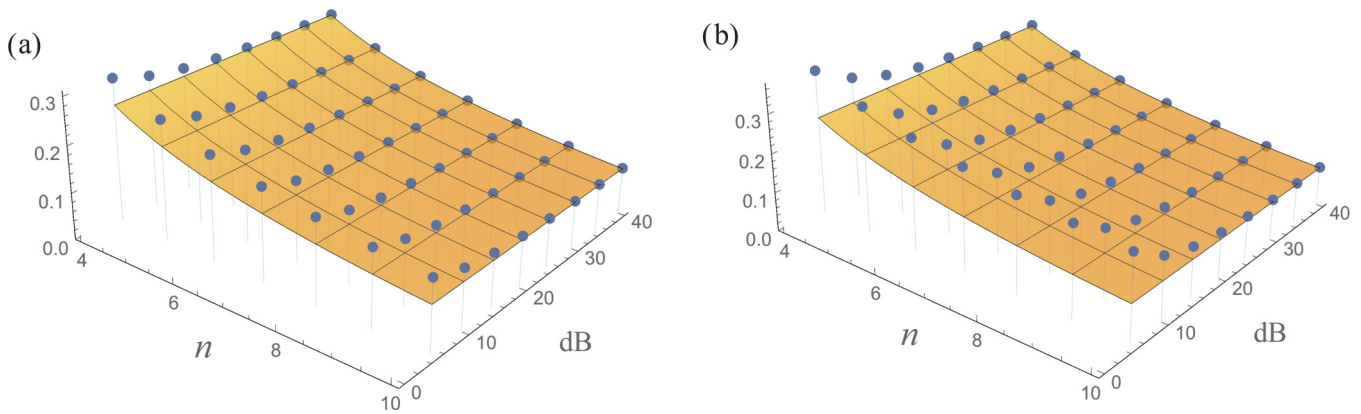

FIG. 3. Average probability that the broadcaster is correctly identified in a single-shot broadcast of exactly one bit of data (i.e., only the sign of the broadcast message is recorded). The dots are plots of the probability to guess correctly, Eq. (66), for various values of n and amounts of squeezing (in dB), with a wedge width $w = 6$. The orange plane is $1/n$, which corresponds to uniformly random guessing. The broadcast magnitude r_0 is scaled according to Eq. (48) to correspond to (a) 1% probability of bit-flip error and (b) 0.0001% probability of bit-flip error.

The most important thing to note from these plots is that for large squeezing, the probability of correctly guessing the broadcaster $\sim 1/n$, which is no better than guessing randomly. Also note that for low squeezing, requiring a lower $p_{\rm err}$ (the chance of a bit flip in the message) increases the risk that the broadcaster is correctly identified. This is consistent with the tradeoff we found between channel capacity and anonymity in the asymptotic analysis of Sec. V. Ideally, we would like to be able to see whether the same phenomenon appears for large n in this case that we found in the asymptotic analysis—i.e., increased risk of detection for large n. Because of numerical limitations, we were unable to evaluate this case for large n, so we leave this as an open question.

VII. ERROR MITIGATION BY RESERVOIR ENGINEERING

After preparation, a CV toric-code state can be protected from errors arising from decoherence and other sources while the players await the broadcasting protocol. Here we present a proof-of-principle calculation to illustrate the method; we leave a full derivation to a future publication.

For simplicity, we focus on creating the toric-code logical vacuum state $|{\rm GS}_{\rm vac}\rangle$, Eq. (12). Note that this is not the same as the state used in the analysis of the broadcasting protocol above—that being the toric-code logical squeezed state $|{\rm GS}_{\rm sq}\rangle$, Eq. (12). We choose the vacuum state, however, because it most clearly illustrates the basics of the method, which relies on reservoir engineering [32], where a dynamical master equation typically drives the system towards a desired steady state.

This is achieved by coupling the physical modes to bosonic reservoirs, $\{\hat{b}_i(\omega)\}$, at each vertex and face of the lattice; see Fig. 1(d). The mode-reservoir coupling is described by a quadratic, quasi-local Hamiltonian

$$\hat{H}_{\rm int} = \sum_{i\in\{\mathcal{V},\mathcal{F}\}} \int d\omega\, \kappa(\omega)[\hat{\eta}_i \hat{b}_i^\dagger(\omega) + \hat{\eta}_i^\dagger \hat{b}_i(\omega)], \tag{67}$$

where $[\hat{b}_i(\omega),\hat{b}_j^\dagger(\omega')] = \delta_{i,j}\delta(\omega-\omega')$. Tracing out the reservoirs in the usual Markov and rotating-wave approximations yields a map in Lindblad form with the CV toric-code nullifiers $\hat{\eta}_i$ as jump operators,

$$\mathcal{L}_{\rm cool}[\hat{\rho}] = \sum_{i\in\{\mathcal{V},\mathcal{F}\}} \left(\hat{\eta}_i \hat{\rho} \hat{\eta}_i^\dagger - \frac{1}{2}\{\hat{\eta}_i^\dagger \hat{\eta}_i, \hat{\rho}\}_+\right), \tag{68}$$

and decay rate $\gamma_{\rm cool} = 2\pi|\kappa(\omega_0)|^2$ arising from evaluation of the coupling strength at frequency ω_0 [33]. For finite squeezing, the nullifiers in Eqs. (6) are not Hermitian, and the map in Eq. (68) cools by extracting entropy from the Hilbert space spanned by the nullifiers. The map in Eq. (68) drives the state toward the code space (i.e., the nullspace of the nullifiers), $\hat{\rho} \to \hat{\rho}_{\rm GS} = |\boldsymbol{\eta}\rangle\langle\boldsymbol{\eta}|_{\rm null} \otimes \hat{\rho}_{\mathcal{L}}$, where $\hat{\rho}_{\mathcal{L}}$ is in general a mixed state in the logical modes that depends on the initial state.

During maintenance of a CV toric code, the cooling provided by Eq. (68) competes against errors. A local error, e.g., photon loss on a single mode, takes the system outside the null space of some or all of the nullifiers touching that mode. The map in Eq. (68) returns the state to the code space at the expense of mixedness within the logical modes. To illustrate performance, we assume local photon loss with a uniform rate for all modes, although such cooling can be effective against more general errors including those that are asymmetric, nonlocal, and correlated.

Here, we consider the evolution of the state of the collection of modes, $\hat{\rho}$, under the cooling in Eq. (68) while each physical mode is subject to photon loss at rate $\gamma_{\rm loss}$. These dynamics are described by the master equation

$$\frac{d}{dt}\hat{\rho} = \gamma_{\rm cool}\mathcal{L}_{\rm cool}[\hat{\rho}] + \gamma_{\rm loss}\sum_{e\in\mathcal{E}}\left(\hat{a}_e\hat{\rho}\hat{a}_e^\dagger - \frac{1}{2}\{\hat{a}_e^\dagger\hat{a}_e,\hat{\rho}\}_+\right). \tag{69}$$

The cooling map in Eq. (68), which is implemented quasilocally, damps out unwanted errors. Since such error protection is not active error correction, we refer to it as *mitigation*.

In order to keep the focus of this work on the broadcasting protocol, we defer the details of this mitigation process to a separate publication. To illustrate the benefit of this method, however, we begin with a CV toric-code vacuum state $|{\rm GS}_{\rm vac}\rangle$ from Eq. (12) using the symmetric nullifiers from Eqs. (6). This state then undergoes simultaneous local loss with rate $\gamma_{\rm loss}$. Local loss leads to the state decaying to the local vacuum of all modes, but this process can be kept in check by error mitigation as shown in Fig. 4.

For Gaussian dynamics, the evolution can be described entirely by the quadrature means and covariance matrix as described in Appendix D. We quantify the performance of the error mitigation by the Uhlmann-Jozsa fidelity [34],

$$\mathcal{F}(\hat{\rho},\hat{\sigma}) = \left[{\rm tr}\left(\sqrt{\sqrt{\hat{\rho}}\hat{\sigma}\sqrt{\hat{\rho}}}\right)\right]^2. \tag{70}$$

For the pure target state $\hat{\sigma} = |{\rm GS}_{\rm vac}\rangle\langle{\rm GS}_{\rm vac}|$, the fidelity reduces to $\mathcal{F}(\hat{\rho},\hat{\sigma}) = {\rm tr}(\hat{\rho}\hat{\sigma})$, which can be evaluated directly from the covariance matrices using the formula $\mathcal{F}(\hat{\rho},\hat{\sigma}) = [\det(\boldsymbol{\Sigma}+\boldsymbol{\Sigma}_\sigma)]^{-1/2}$ [35]. Figure 4(a) shows the improved fidelity for increasing cooling rates, illustrating error mitigation.

All CV toric-code states satisfy the condition that $\hat{\eta}_i|{\rm GS}\rangle = 0$ for all nullifiers. A measure of the degree to which this condition is violated, and thus the degree to which the state leaves the code space, is the nullifier excitation number $\langle\hat{\eta}^\dagger\hat{\eta}\rangle$. Figure 4(b) shows the protection of the code space as the nullifier excitation number is stabilized by the cooling map, Eq. (68). After a relaxation time that scales with the lattice size, the system approaches a steady state. For strong cooling, $\gamma_{\rm loss}/\gamma_{\rm cool} \ll 1$, one finds that the expectation value of the nullifier number operators reaches a steady-state (ss) value that scales $\langle\hat{\eta}_v^\dagger\hat{\eta}_v\rangle_{\rm ss} = \langle\hat{\eta}_f^\dagger\hat{\eta}_f\rangle_{\rm ss} \propto \gamma_{\rm loss}/\gamma_{\rm cool}$. Thus, the steady state is close to the toric-code vacuum, $\hat{\rho}_{\rm ss} \sim |{\rm GS}_{\rm vac}\rangle\langle{\rm GS}_{\rm vac}|$.

VIII. OPTICAL IMPLEMENTATION

This protocol may be implemented using recently demonstrated methods for generating large-scale optical CV cluster

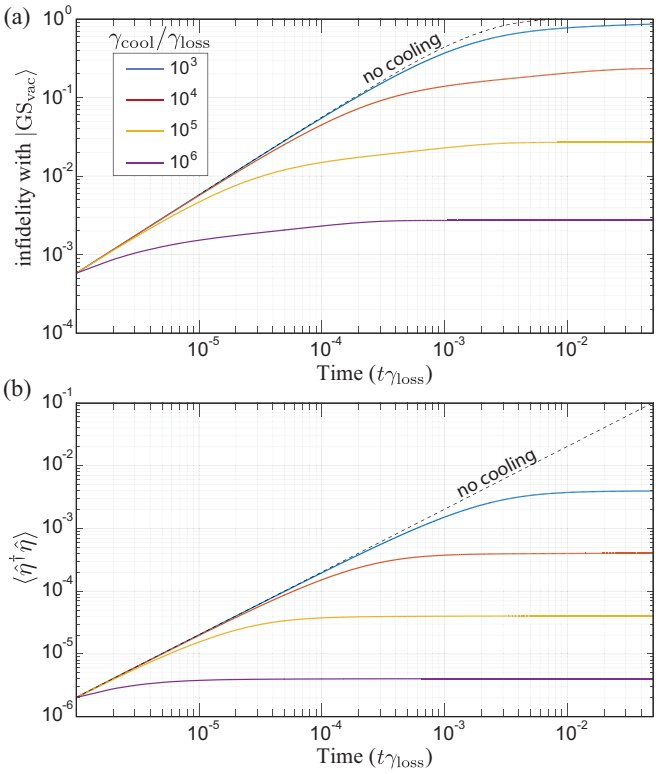

FIG. 4. Example of state maintenance via dissipative error mitigation. The initial state is the CV toric-code vacuum $|{\rm GS}_{\rm vac}\rangle$, Eq. (12), defined by the symmetric nullifiers, Eqs. (6), on a 6×24 lattice with 10 dB of squeezing ($s=\sqrt{10}$). (a) Infidelity with $|{\rm GS}_{\rm vac}\rangle$, $1-\mathcal{F}(\hat{\rho},\hat{\sigma})$, where fidelity is given by Eq. (70). (b) Excitation number, $\langle\hat{\eta}^\dagger\hat{\eta}\rangle$, for a single nullifier (identical for face or vertex). In both (a) and (b), the curves are ordered $\gamma_{\rm cool}/\gamma_{\rm loss}=\{10^3,10^4,10^5,10^6\}$ from top to bottom.

states encoded in either frequency modes [36,37] or temporal modes [38,39]. The GHZ-state version is achievable now with achieved squeezing levels (5 dB) in current technology [39]. Proof-of-principle experiments with a surface-code state are possible with ∼10 dB of squeezing, which is state of the art but achievable [39–41]. Higher squeezing would enable practical large-scale anonymous broadcasting.

Resource states could also be prepared in circuit-QED setups, either dynamically or by engineering a quadratic Hamiltonian between microwave cavities [42] that has the CV cluster state as the gapped ground state and then performing quadrature measurements to map it to a CV surface code [16]. Single-mode [43,44] and two-mode [45–48] squeezing has already been demonstrated in these systems, and the SQUID-based[4] controlling technology allows for very strong nonlinearities [49–51], enabling high squeezing (∼13 dB) [52–56].

A. Macrocode-based CV cluster states

Recent experimental results have shown that compact optical experimental setups can produce huge CV cluster states, including million-mode [57] and 10^4-mode CV cluster states [39] with modes multiplexed in time (temporal modes) and a 60-mode CV cluster state [37] with modes multiplexed in frequency (frequency modes). These are cluster states with linear graphs, but the extension to a square lattice is straightforward and readily achievable with current technology [36,58,59].

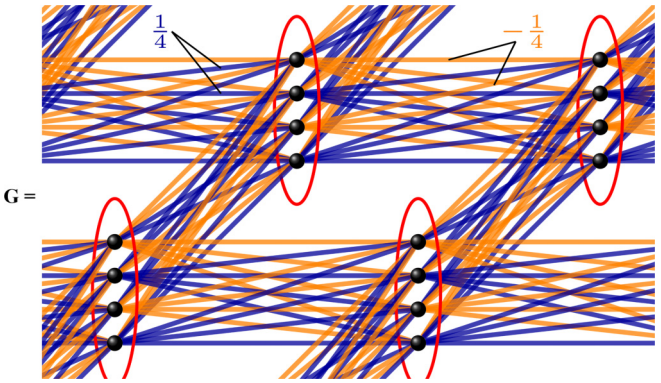

FIG. 5. Basic graph **G** for temporal-mode CV cluster states [38]; the full graph [58] is given in Eq. (71). **G**, as shown, also represents frequency-mode CV cluster states [36,59,60] up to trivial π phase shifts that merely flip the sign of some of the edges. Notice that **G** has the overall structure of a square lattice, but the individual nodes of that lattice are now collections of four nodes called *macrocodes*. Each macronode is identified by its surrounding red oval. In the temporal-mode case [38], each of the four nodes within a macronode is a synchronous temporal mode in four spatially separate laser beams. In the cylindrical frequency-mode case [36], each of the four nodes within a macronode share a common frequency but differ in spatial beam and polarization. The toroidal frequency-mode case [59,60] is more complicated in structure and offers no advantages over the cylindrical one, so we do not consider it further.

These setups were already discussed in Ref. [16] as candidates for generating CV surface-code states like the ones necessary for this protocol. Here we review this construction and discuss its implementation for anonymous broadcasting.

The temporal-mode [38,39] and frequency-mode [36,37,59,60] construction methods generate a toroidal [59,60] or cylindrical [36,38] CV cluster state with a Gaussian graph [58] whose overall structure is that of a square lattice but is nevertheless not an ordinary square lattice. Instead, it is a lattice based on four-node groupings called *macronodes*, with a structure as shown in Fig. 5. The actual CV cluster state has the full graph [58]

$$\mathbf{Z}=i\delta\mathbf{I}+t\mathbf{G}, \tag{71}$$

where $\delta=\operatorname{sech}2r$, $t=\tanh 2r$, and **G** is the graph shown in Fig. 5, with edge weights $\pm\frac{1}{4}$.

By measuring the top three modes of each macronode in $\hat{q}$, all but a single layer of the grid is deleted, leaving a uniformly weighted, ordinary CV cluster state with graph [58]

$$\mathbf{Z}_{\rm CS}=i\delta\mathbf{I}+g\mathbf{A}_{\rm grid}, \tag{72}$$

where $\delta=\operatorname{sech}2r$, $g=\frac{1}{4}\tanh 2r$, $r>0$ is an overall squeezing parameter, and $\mathbf{A}_{\rm grid}$ is a binary adjacency matrix for an ordinary square-lattice graph with boundary conditions

[4]Note: "SQUID" stands for "superconducting quantum interference device."

(toroidal or cylindrical) inherited from its parent, Eq. (71). Note that the edge weights in $\mathbf{Z}_{\mathrm{CS}}$ are all $\frac{1}{4}\tanh 2r$, while in the canonical construction, they should all be 1. Nevertheless, we can remodel the cluster state [16,61] by redefining quadratures so that the edge weights are 1 but at a cost of multiplying the self-loop weights by g^{-1}. Since $\operatorname{sech} 2r = \delta =: s_0^{-2}$, this means that the original value of s_0 (so labeled to differentiate it from the actual s used in the protocol) could be considered to be $s_0 = \sqrt{\cosh 2r}$, except for the nonunit g. The new effective value of s, which should be used in the calculations in the previous sections, is less than half this initial value [16,61]:

$$s = \frac{s_0}{2}\sqrt{\tanh 2r} = \frac{1}{2}\sqrt{\sinh 2r}. \tag{73}$$

With a canonical CV cluster state obtained, which has uniform edge weight of 1, with s from Eq. (73), we can use local $\hat{q}$ measurements to "cut and unroll" the cylinder or torus into a square lattice with the necessary smooth/rough boundary conditions as identified in Appendix A 6. Further local $\hat{q}$ and $\hat{p}$ measurements are then used to convert this state to a CV surface code state [16] with two rough and two smooth edges as shown in Fig. 9(b), which is then distributed to the players. The broadcast protocol proceeds according to the modifications described in Appendix A 6.

One might think we could take advantage of the cylindrical or toroidal structure of the original CV cluster states to produce a surface-code state with periodic boundaries. This fails, however, because the graphs of both states have a one-grid-unit twist along each compactified direction [36,38,60], which makes the checkerboard pattern of measurements needed to convert it into a cylindrical or toroidal surface code fail to line up properly. This is why we have to cut it into a surface code with open boundaries instead. If the twist were by an even number of grid units, other boundary conditions might be possible.

The temporal-mode scheme [38] claims an advantage over the cylindrical frequency-mode scheme [36] in terms of ease of distribution. This is because the temporal-mode cylindrical lattice is built up like sequentially winding thread around a spool. This means that large chunks of the lattice are contiguous in time. Thus, one only needs a quickly adjustable mirror in order to distribute the pieces of the lattice to the players. Initially, the mirror is used to direct one of the four output beams to the first player. (The other three beams are immediately measured in $\hat{q}$ to do the projection down to an ordinary lattice.) Once the player has received enough modes to form his or her sublattice, the mirror is switched so that the output beam is directed toward the second player, and so on. $\hat{q}$ measurements at the start and end of this entire process are used to clean up the total lattice before the players themselves do the necessary additional $\hat{q}$ and $\hat{p}$ measurements to transform the state into a surface-code state. The "radius of the cylinder" in the temporal-mode case is limited by the coherence length L of the laser, but its width in the temporal direction—which is the direction used to measure the width w of each player's wedge, for instance—is not so limited since far-separated modes do not need to directly interact. This means that the temporal-mode scheme is capable of involving a practically unlimited number of players.

The cylindrical frequency-mode scheme [36] has the same graph structure, but the frequencies of nearby modes are widely separated, so it is not as easy to split the lattice up into contiguous pieces for distribution. If this hurdle could be overcome, the frequency-mode scheme might claim an advantage because it is a continuous-wave scheme, meaning it might provide a means to transmit information continuously, rather than in bursts, as would be required by the temporal-mode scheme.

B. Squeezing levels for surface-code protocol

The rescaling of s shown in Eq. (73) means that this is likely not the most efficient way of generating a surface-code state, in terms of making good use of available squeezing resources [61]. Further theoretical work could lead to better procedures, but for now, we can look at the state of the art and what is achievable.

The largest squeezing achieved to date in these large-scale schemes is 5 dB in the temporal-mode experiment [39]. This corresponds to[5]

$$r = \frac{\#\mathrm{dB}}{20}\ln 10 \simeq 0.5756, \tag{74}$$

which means that the effective s for a protocol using this state is

$$s = \tfrac{1}{2}\sqrt{\sinh 2r} \simeq 0.5965, \tag{75}$$

which corresponds to an effective initial squeezing of

$$(\text{effective } \#\mathrm{dB}) = 20\log_{10} s \simeq -4.488\ \mathrm{dB} \tag{76}$$

when doing the protocol. The negative sign means that this state is equivalent to a canonical CV cluster state [Fig. 7(a)] made with *antisqueezed* vacuum modes (i.e., vacuum modes squeezed in the wrong direction) [58]. Note that this does not mean that we would be better off not doing any squeezing at all in the actual experiment. Instead, this is simply a side effect of the straightforward, but squeezing-inefficient [16,61], projection to an ordinary lattice from the macrocode-based lattice shown in Fig. 5. In this case, it produces a poor-quality state that is equivalent to one made with antisqueezed input modes. Since we want $s^2 \gg 1$ for nontrivial channel capacity with high anonymity, either improved squeezing or further theoretical improvements in the protocol would be required to make practical use of these resources.

Single-mode squeezing as high as 12.7 dB [40,41], and even 15 dB [62], has been achieved in optics experiments, so it would be state of the art, but not unreasonable, to consider 10 dB achievable in temporal-mode [38,39] or frequency-mode [36,37] CV cluster states. Using Eqs. (74), (75), and (76), this corresponds to an effective squeezing of $+0.925$ dB, or an effective $s = 1.112$. This would still allow for semianonymous broadcasting—which we define as giving a probability $p < 2/n$ of the sender being correctly identified (less than twice the probability of random guessing). This would be possible when broadcasting 0.25 bits (corresponding to an SNR $\alpha = 0.414$) for $n \leqslant 11$ or broadcasting 0.5 bits ($\alpha = 1$) with $n \leqslant 5$. This would be enough for a proof-of-principle demonstration.

[5]Here and throughout, the abbreviation "#dB" stands for "number of decibels."

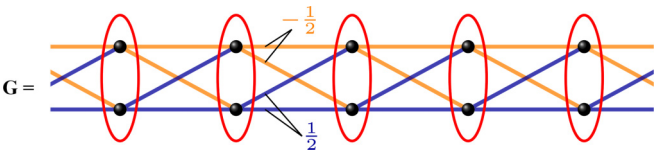

FIG. 6. Basic graph **G** for the temporal-mode linear CV cluster state reported in Ref. [39]; the full graph **Z** [58] is obtained from this through Eq. (71). **G**, as shown, also represents frequency-mode CV cluster states reported in Ref. [37] up to trivial π phase shifts that merely flip the sign of some of the edges. Notice that **G** has the overall structure of a line graph, but the individual nodes of that lattice are now collections of two nodes called *macrocodes*. Each macronode is identified by its surrounding red oval. In the temporal-mode experiment [38,39], each node within a macronode is a synchronous temporal mode in spatially separate laser beams. In the frequency-mode experiment [36,37], each node is one of two polarizations with the same frequency.

C. Squeezing levels for GHZ-state protocol

The calculations above assume that a full surface-code state is used as the resource. This has a macrocode-based graph with edge weights $\pm\frac{1}{4}$, as shown in Fig. 5, which reduces the effective squeezing dramatically when projected down to an ordinary lattice [61]. A surface code is necessary for error mitigation but not for basic demonstration of the protocol itself. For this, a simple GHZ state will suffice. As shown in Appendix A 4, this can be made from a linear CV cluster state.

The basic graph **G** for the actual state created in the temporal-mode experiment [39] is shown in Fig. 6, where the full graph **Z** [58] is again obtained from **G** through Eq. (71). This graph has two-node macrocodes (instead of four-node), and the edge weights are $\pm\frac{1}{2}$ (instead of $\pm\frac{1}{4}$), which means that with a base squeezing of 5 dB, the effective s for a protocol based on this linear resource [61] is larger than in the surface-code case [compare Eq. (75)]:

$$r \simeq 0.5756 \quad \Longrightarrow \quad s = \frac{1}{\sqrt{2}}\sqrt{\sinh 2r} \simeq 1.006. \tag{77}$$

This corresponds to an effective initial squeezing of

$$(\text{effective \#dB}) = 20\log_{10} s \simeq +0.05297\ \text{dB}, \tag{78}$$

which can be compared with Eq. (76).

With error correction not possible when using a GHZ state, we can reduce the wedge width w to its minimum value: $w = 1$. In this scenario, semianonymous broadcasting ($p < 2/n$; see subsection above) is possible for

$$C = 0.25\,\text{bits} \quad (\alpha = 0.414), \quad n \leqslant 17; \tag{79}$$

$$C = 0.5\,\text{bits} \quad (\alpha = 1), \quad n \leqslant 8; \tag{80}$$

$$C = 0.75\,\text{bits} \quad (\alpha = 1.828), \quad n \leqslant 5; \tag{81}$$

$$C = 1\,\text{bit} \quad (\alpha = 3), \quad n \leqslant 4. \tag{82}$$

Thus, optical technology available today [39] can be used to demonstrate a practical implementation of GHZ-state-based anonymous broadcasting using this protocol.

D. Scalability

The main advantage of these optical implementations remains in their immense scalability. CV GHZ states are already available today with current technology for anonymous broadcasting, and surface-code-based protocols are possible with state-of-the-art implementations. If the squeezing can be increased (or a more efficient conversion protocol devised), this technology holds great promise for large-scale anonymous broadcasting.

IX. CONCLUSION

We propose using large-scale continuous-variable topological quantum codes for the important practical task of anonymously broadcasting classical information, and we quantify the channel capacity and anonymity of the protocol in terms of its physical parameters. Large squeezing enables high-capacity broadcasting with strong anonymity, but there is a tradeoff between the two for any fixed level of squeezing. Our protocol outperforms other anonymous broadcasting protocols in two crucial ways: (1) Because a topological quantum code serves as the resource, the scheme is robust to errors and further can be protected with quasilocal reservoir engineering. (2) Because that code is a continuous-variable code, the technology required for large-scale resource generation is already available. A notable feature of our protocol using continuous variables (instead of qubits) is that with sufficiently large squeezing, anonymity is maintained even with channel capacity $C > 1$ bit. This would enable other, more complex tasks such as anonymous yes-or-no voting [6,63] within a group of size $\leqslant C$.

ACKNOWLEDGMENTS

G.K.B. thanks James Wootton for discussions on the discrete variable protocol and thanks J. Dowling for comments. T.F.D. thanks Joseph Fitzsimons for useful suggestions about past work on anonymous communication. B.Q.B. thanks Naoki Yamamoto and Ian Petersen for valuable comments. N.C.M. thanks Marco Tomamichel for useful discussions. T.F.D. is supported by the Singapore National Research Foundation under NRF Award No. NRF-NRFF2013-01. N.C.M. is supported by the Australian Research Council (ARC) under Grant No. DE120102204 and by the U.S. Defense Advanced Research Projects Agency (DARPA) Quiness program under Grant No. W31P4Q-15-1-0004. N.C.M. and B.Q.B acknowledge support from the ARC Centre of Excellence for Quantum Computation and Communication Technology (Project No. CE170100012). G.K.B., T.F.D., and B.Q.B. acknowledge support from the ARC Centre of Excellence for Engineered Quantum Systems (Project No. CE110001013). G.K.B. acknowledges support from ARC Project No. DP160102426.

APPENDIX A: PLAYERS' COVARIANCE MATRIX (BEFORE BROADCAST)

In this section, we calculate the covariance matrix and associated statistics of the players' measurements of the string momentum operator $\hat{M}$ corresponding to the initial state, that is, *before* any broadcast is sent.

1. Preparation by measurement of a CV cluster state

A CV toric-code state can be prepared from a CV cluster state using local measurements, as described in Ref. [16]. Given the exact nullifiers for a finitely squeezed CV cluster state on a square lattice (specifically, a weight-1, canonical CV cluster state) [58],

$$\hat{\eta}_j^{\mathrm{CS}} = \frac{1}{\sqrt{2}}\left[s^{-1}\hat{q}_j + is\left(\hat{p}_j - \sum_{k\in\mathcal{N}(j)}\hat{q}_k\right)\right], \tag{A1}$$

the measured modes lie on the vertices and the face centers of graph for the CV surface-code state, while the unmeasured nullifiers lie on the edges [see Figs. 1(b) and 7]. Consider an alternating sum of cluster-state nullifiers $\hat{\eta}_j^{\mathrm{CS}}$ centered on the nodes of a loop $\mathcal{P}$ [e.g., every other node left to right through the middle of Fig. 7(a): . . . ,72, 98, . . .]. This sum is also a nullifier of the original CV cluster state. The overlapping $\hat{q}$ terms have canceled, and the sum can be written (up to normalization) as

$$\frac{-i}{\sqrt{|\mathcal{P}|}}\sum_{e_k\in\mathcal{P}}(-1)^k\hat{\eta}_k^{\mathrm{CS}} = \hat{f} - \frac{s}{\sqrt{2|\mathcal{P}|}}\sum_{e_k\in\mathcal{P}}\left(\hat{q}_{v_k^L} + \hat{q}_{v_k^R}\right), \tag{A2}$$

where $\hat{q}_{v_k^{L(R)}}$ are the position operators for the modes to the left (right) of the edge e_k with respect to $\mathcal{P}$, and they are located at the faces of the CV toric code (e.g., nodes 71, 73, 97, 99). We have defined the string operator $\hat{f}$ around the loop $\mathcal{P}$,

$$\hat{f} := \frac{1}{\sqrt{2|\mathcal{P}|}}\sum_{e\in\mathcal{P}} o(e)(s\,\hat{p}_e - is^{-1}\hat{q}_e), \tag{A3}$$

where $|\mathcal{P}|$ is the loop length and $o(e) = \pm 1$ if edge e is oriented in the same (opposite) direction as $\mathcal{P}$.

Since these modes are measured in the $\hat{q}$ basis we have a record of their values $\{q_{v_k^L}, q_{v_k^R}\}$. Call the accumulated value

$$Q = \frac{s}{\sqrt{2|\mathcal{P}|}}\sum_{e_k\in\mathcal{P}}\left(q_{v_k^L} + q_{v_k^R}\right). \tag{A4}$$

Then, the prepared state satisfies

$$(\hat{f} - Q)|\mathrm{GS_{sq}}\rangle = 0. \tag{A5}$$

Henceforth, we take $Q = 0$ because the displacement can be accounted for in the protocol by subtracting the value Q when inferring the broadcast message.

2. Logical modes of the finitely squeezed CV toric code

While string operators (complete loops) are exact logical operators in the case of the qubit [12], qudit [19], and ideal (infinitely squeezed) [23] CV toric codes, they are only approximately so in the case of a finitely squeezed CV toric code. This is because, as noted in Eqs. (8), finitely squeezed toric-code nullifiers fail to commute with their daggered neighbours. We can, however, identify a set of modes that commute with all toric-code nullifiers and their daggers.

One possible definition of these two logical modes is

$$\hat{a}_{\mathcal{L},\nearrow} := \frac{1}{\sqrt{N}}\sum_{e\in\mathcal{E}} o_{\nearrow}(e)\hat{a}_e, \tag{A6a}$$

$$\hat{a}_{\mathcal{L},\nwarrow} := \frac{1}{\sqrt{N}}\sum_{e\in\mathcal{E}} o_{\nwarrow}(e)\hat{a}_e, \tag{A6b}$$

where $\mathcal{E}$ is the set of edges in Fig. 1(c), N is the total number of physical modes (note that $|\mathcal{E}| = N$), and (recalling that the CV toric code is defined on an oriented lattice)

$$o_{\nearrow}(e) := \begin{cases} +1 & \text{if edge } e \text{ is oriented } \uparrow \text{ or } \rightarrow, \\ -1 & \text{if edge } e \text{ is oriented } \downarrow \text{ or } \leftarrow, \end{cases} \tag{A7a}$$

$$o_{\nwarrow}(e) := \begin{cases} +1 & \text{if edge } e \text{ is oriented } \uparrow \text{ or } \leftarrow, \\ -1 & \text{if edge } e \text{ is oriented } \downarrow \text{ or } \rightarrow. \end{cases} \tag{A7b}$$

The subscript $\nearrow$ or $\nwarrow$ on o is chosen to make this definition intuitive. This results, as can be seen from the orientations of the edges in Fig. 1(c), in two operators formed as linear combinations of the physical modes, with signs that alternate along one of the two diagonals and are constant on the other. In fact, the mode shape corresponds to the highest spatial-frequency standing-wave modes commensurate with the lattice in the two diagonal directions. The two logical mode operators are canonical—i.e., $[\hat{a}_{\mathcal{L},i}, \hat{a}^\dagger_{\mathcal{L},j}] = \delta_{ij}$, where $i, j \in \{\nearrow, \nwarrow\}$. They satisfy

$$\hat{a}_{\mathcal{L},\nearrow}|\mathrm{GS_{vac}}\rangle = \hat{a}_{\mathcal{L},\nwarrow}|\mathrm{GS_{vac}}\rangle = 0. \tag{A8}$$

By taking linear combinations, we can define operators that have support only on vertical and horizontal edges—i.e.,

$$\hat{a}_{\mathcal{L},\uparrow} := \frac{1}{\sqrt{2}}(\hat{a}_{\mathcal{L},\nearrow} + \hat{a}_{\mathcal{L},\nwarrow}) = \sqrt{\frac{2}{N}}\sum_{e\in\mathcal{E}_\updownarrow} o_{\uparrow}(e)\hat{a}_e, \tag{A9a}$$

$$\hat{a}_{\mathcal{L},\rightarrow} := \frac{1}{\sqrt{2}}(\hat{a}_{\mathcal{L},\nearrow} - \hat{a}_{\mathcal{L},\nwarrow}) = \sqrt{\frac{2}{N}}\sum_{e\in\mathcal{E}_\leftrightarrow} o_{\rightarrow}(e)\hat{a}_e, \tag{A9b}$$

respectively, where the subscript $\updownarrow$ ($\leftrightarrow$) on $\mathcal{E}$ restricts the set to only those edges that are vertical (horizontal), and where the o functions are ± 1 if the orientation of e is the same (opposite) of the arrow in the subscript. Examining Fig. 1(c), we see that both of these modes have signs alternating in a checkerboard pattern.

The important difference between this situation and that of the qubit [12], qudit [19], or ideal CV [23] toric code is that the exact logical modes defined in Eqs. (A9) are linear combinations of *all* string modes along the same direction. Individual string modes are now *approximate* logical modes, with the approximation improving as the squeezing factor s increases.

A full description of the finitely squeezed CV toric code will presented in a separate publication. We conclude this subsection by justifying the description of the CV toric-code ground states presented in Sec. III A.

First, one can explicitly verify that any of the modes defined above commute with all nullifiers and with their daggers—both in the symmetric case [Eqs. (6)] and in the asymmetric case [16], which is further discussed below. The logical modes are related to the physical modes by a passive transformation, which means that the simultaneous vacuum state of all physical modes is also vacuum in the logical subspace, thereby justifying Eqs. (11) and (12).

We now repeat the analysis of Appendix A 1—which applies to the CV toric-code state obtained by measuring a CV cluster state [16]—using these logical modes instead of

individual string modes. We find

$$\hat{f}_{\nearrow} := \frac{-i}{\sqrt{N}} \sum_{e_k \in \mathcal{E}} o_{\nearrow}(e_k) \hat{\eta}_k^{\mathrm{CS}}$$
$$= \frac{1}{\sqrt{2N}} \sum_{e \in \mathcal{E}} o_{\nearrow}(e)(s\hat{p}_e - is^{-1}\hat{q}_e), \quad \text{(A10a)}$$
$$\hat{f}_{\nwarrow} := \frac{-i}{\sqrt{N}} \sum_{e_k \in \mathcal{E}} o_{\nwarrow}(e_k) \hat{\eta}_k^{\mathrm{CS}}$$
$$= \frac{1}{\sqrt{2N}} \sum_{e \in \mathcal{E}} o_{\nwarrow}(e)(s\hat{p}_e - is^{-1}\hat{q}_e), \quad \text{(A10b)}$$

and therefore

$$\hat{f}_{\nearrow}|\mathrm{GS_{sq}}\rangle = \hat{f}_{\nwarrow}|\mathrm{GS_{sq}}\rangle = 0. \quad \text{(A11)}$$

Note that by including all unmeasured modes, we have eliminated the dependence on the measurement outcomes [compare with Eq. (A5)]. Also notice that $\hat{f}_{\nearrow}$ and $\hat{f}_{\nwarrow}$ are merely (up to a phase) squeezed versions of $\hat{a}_{\mathcal{L},\nearrow}$ and $\hat{a}_{\mathcal{L},\nwarrow}$, respectively, with squeezing factor s. This justifies Eq. (13).

Finally, note that

$$(\alpha \hat{a}_{\mathcal{L},\nearrow} + \beta \hat{a}_{\mathcal{L},\nwarrow})|\mathrm{GS_{vac}}\rangle = 0, \quad \text{(A12)}$$
$$(\alpha \hat{f}_{\nearrow} + \beta \hat{f}_{\nwarrow})|\mathrm{GS_{sq}}\rangle = 0, \quad \text{(A13)}$$

$\forall \alpha, \beta \in \mathbb{C}$. Therefore, expressing $|\mathrm{GS_{vac}}\rangle$ or $|\mathrm{GS_{sq}}\rangle$ in a different set of modes within the logical subspace will also have the same form as long as those modes are related to the original ones by a passive transformation.

3. General formulation

We prepare a finitely squeezed CV toric code via measurements on a canonical CV cluster state, as described in Ref. [16]. In this case, the CV toric-code face nullifiers are unchanged, but the vertex nullifiers deviate slightly from the symmetric nullifiers defined in Eqs. (6). These *asymmetric* nullifiers are

$$\hat{\tilde{\eta}}_v := \frac{1}{\sqrt{8}} \left[\sum_{e \in +_v} \left(\tilde{s}\hat{q}_e + i\tilde{s}^{-1}\hat{p}_e \right) + s^2 \tilde{s}^{-1} \sum_{e \in \Diamond_v} \hat{q}_e \right], \quad \text{(A14a)}$$
$$\hat{\tilde{\eta}}_f := \frac{1}{\sqrt{8}} \sum_{e \in \square_f} o(e,f)(s\hat{p}_e - is^{-1}\hat{q}_e) \quad \text{(A14b)}$$

(with some simple modifications if on a surface with boundary), where $\tilde{s} = \sqrt{5s^2 + s^{-2}}$, and $\Diamond_v$ means the diamond shaped loop of next nearest neighbors to the vertex v [16].

Figure 6 of Ref. [16] shows the Gaussian graph [58] for the CV surface code state $|\mathrm{GS_{sq}}\rangle$ created from a canonical CV cluster state, which is also reproduced here in Figure 7(b). Since its graph $\mathbf{Z} = i\mathbf{U}$ is purely imaginary, it directly encodes the pp correlations [58]: $\langle \hat{\mathbf{p}}\hat{\mathbf{p}}^{\mathrm{T}} \rangle = \frac{1}{2}\mathbf{U}$.

When using this state for anonymous broadcasting, $\mathcal{P}$ is left to right along one of these horizontal lines—e.g., $\ldots, 72, 98, \ldots$ in Fig. 7(b). We can write each player's measurement operator $\hat{M}_j$ along a portion $\mathcal{P}_j$ of this path as the inner product between the vector of momentum operators $\hat{\mathbf{p}}$ and a normalized indicator vector $\boldsymbol{\ell}_j = |\mathcal{P}_j|^{-1/2}\boldsymbol{\lambda}_j$, where all entries of $\boldsymbol{\lambda}_j$ are ± 1 or 0. Assuming the width of each wedge is w, then the portion of the string momentum, Eq. (18), can be expressed as

$$\hat{M}_j = \boldsymbol{\ell}_j^{\mathrm{T}} \hat{\mathbf{p}} = \frac{1}{\sqrt{w}} \boldsymbol{\lambda}_j^{\mathrm{T}} \hat{\mathbf{p}}. \quad \text{(A15)}$$

With respect to the initial state (i.e., before any displacements intended to broadcast a message),

$$\langle \hat{M}_j \hat{M}_k \rangle = \boldsymbol{\ell}_j^{\mathrm{T}} \langle \hat{\mathbf{p}}\hat{\mathbf{p}}^{\mathrm{T}} \rangle \boldsymbol{\ell}_k = \frac{1}{w} \boldsymbol{\lambda}_j^{\mathrm{T}} \left(\frac{1}{2}\mathbf{U} \right) \boldsymbol{\lambda}_k = \frac{1}{2w} \mathrm{tr}\left(\mathbf{U} \boldsymbol{\lambda}_k \boldsymbol{\lambda}_j^{\mathrm{T}} \right). \quad \text{(A16)}$$

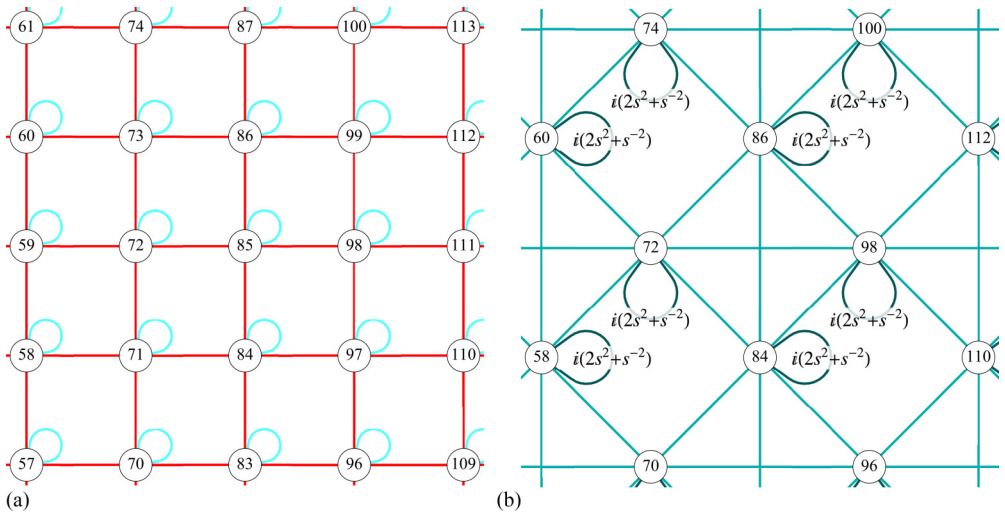

FIG. 7. Toroidal CV cluster state and toroidal CV surface-code state $|\mathrm{GS_{sq}}\rangle$ [16]. (a) Portion of a CV cluster state with toroidal boundary conditions. Red edges have weight 1, and cyan self-loops have weight is^{-2} [58]. (b) Portion of a CV surface-code state with toroidal boundary conditions (CV toric-code state). Unlabeled edges all have weight is^2. This state is generated by measuring $\hat{p}$ and $\hat{q}$ on the odd nodes of panel (a) in a diagonally alternating pattern. The $\hat{p}$ measurements delete the node and produce a criss-cross pattern in panel (b) where the node used to be. The $\hat{q}$ measurements just delete the node. (In this case, $\hat{q}$ was measured on nodes 71, 73, 97, 99; $\hat{p}$ was measured on the other visible odd-numbered nodes; and so on.)

We can also consider the total string momentum measurement $\hat{M} = \boldsymbol{\ell}^{\mathrm{T}}\hat{\mathbf{p}} = |\mathcal{P}|^{-1/2}\boldsymbol{\lambda}^{\mathrm{T}}\hat{\mathbf{p}}$. Assuming n players and a width-w wedge given to each player,

$$(\Delta M)^2 := \langle \hat{M}^2 \rangle = \frac{1}{2nw}\,\mathrm{tr}(\mathbf{U}\boldsymbol{\lambda}\boldsymbol{\lambda}^{\mathrm{T}}). \tag{A17}$$

To illustrate the use of these formulas, it will be instructive to first analyze a simple case.

4. Simple case: Four-mode CV GHZ state

Consider the linear CV cluster state in Fig. 8(a). By measuring $\hat{p}$ on all even nodes, this state becomes the CV GHZ state whose Gaussian graph $\mathbf{Z}$ [58] is shown in Fig. 8(b). Forming its adjacency matrix—also called $\mathbf{Z}$ without ambiguity by taking the nodes in numerical order—we get $\mathbf{Z} = i\mathbf{U}$ with

$$\mathbf{U} = \begin{pmatrix} s^2+s^{-2} & s^2 & 0 & 0 \\ s^2 & 2s^2+s^{-2} & s^2 & 0 \\ 0 & s^2 & 2s^2+s^{-2} & s^2 \\ 0 & 0 & s^2 & s^2+s^{-2} \end{pmatrix}. \tag{A18}$$

We postulate two players using this state for broadcasting with portions of the string momentum, Eq. (A15), given by

$$\hat{M}_1 := \frac{1}{\sqrt{2}}(\hat{p}_1 - \hat{p}_3), \tag{A19}$$

$$\hat{M}_2 := \frac{1}{\sqrt{2}}(\hat{p}_5 - \hat{p}_7), \tag{A20}$$

and total string momentum $\hat{M} = \frac{1}{\sqrt{2}}(\hat{M}_1 + \hat{M}_2)$. Therefore,

$$\boldsymbol{\lambda}_1 = \begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \end{pmatrix}, \quad \boldsymbol{\lambda}_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ -1 \end{pmatrix}. \tag{A21}$$

The trace in Eq. (A16) is the Hilbert-Schmidt inner product (entrywise inner product) between $\mathbf{U}$ and $\boldsymbol{\lambda}_j\boldsymbol{\lambda}_k^{\mathrm{T}}$. The relevant matrices are

$$\boldsymbol{\lambda}_1\boldsymbol{\lambda}_1^{\mathrm{T}} = \begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \tag{A22}$$

$$\boldsymbol{\lambda}_2\boldsymbol{\lambda}_2^{\mathrm{T}} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & 1 \end{pmatrix}, \tag{A23}$$

$$\boldsymbol{\lambda}_1\boldsymbol{\lambda}_2^{\mathrm{T}} = \begin{pmatrix} 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{A24}$$

Taking entrywise inner products of these with $\mathbf{U}$, we find the wedgewise variances,

$$\langle \hat{M}_1^2 \rangle = \langle \hat{M}_2^2 \rangle = \frac{1}{4}[(s^2+s^{-2}) + (2s^2+s^{-2}) - 2s^2] = \frac{s^2}{4} + \frac{1}{2s^2}, \tag{A25}$$

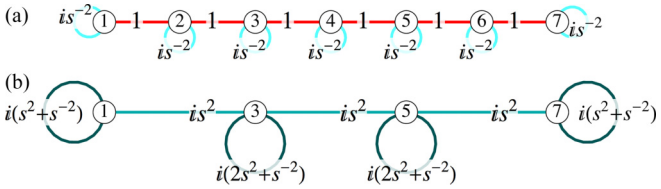

FIG. 8. Graphs for the (a) linear CV cluster state and (b) CV GHZ state, with all edge weights labeled explicitly. Measuring $\hat{p}$ on the even nodes in panel (a) produces panel (b). Notice that the self-loops at the ends of the GHZ state have a different weight from the ones in the middle.

and interwedge covariances,

$$\langle \hat{M}_1\hat{M}_2 \rangle = \langle \hat{M}_2\hat{M}_1 \rangle = \frac{-s^2}{4}. \tag{A26}$$

The total measurement $\hat{M}$ has $\boldsymbol{\lambda} = \boldsymbol{\lambda}_1 + \boldsymbol{\lambda}_2$. Therefore,

$$\boldsymbol{\lambda}\boldsymbol{\lambda}^{\mathrm{T}} = \begin{pmatrix} 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \end{pmatrix}, \tag{A27}$$

and the resultant entrywise inner product with $\mathbf{U}$ is the sum of the diagonal of $\mathbf{U}$ minus all entries on the sub- and superdiagonals:

$$(\Delta M)^2 = \langle \hat{M}^2 \rangle = \frac{1}{8}[2(s^2+s^{-2}) + 2(2s^2+s^{-2}) - 6s^2] = \frac{1}{2s^2}. \tag{A28}$$

Notice that the large-variance terms ($\sim s^2$) cancel in this sum due to the covariances between the wedges, Eq. (A26). (The fact that the self-loops at the ends are different from those in the center of the chain is required for this cancellation to happen.) Therefore, the total string momentum measurement has a small variance even though individual players' measurements have a large variance—this is the essence of the anonymous broadcasting protocol.

5. CV toric-code state

We now return to the case of the toric-code state shown in Fig. 7(b). We assume a general scenario of n players, each of whom possesses a slice of the torus of width w. Because of the toroidal boundary conditions, nw must be even, and we assume it is not trivially small (i.e., $nw \geqslant 4$).

For illustration, we start with the concrete example of $w = 4$. Then,

$$\boldsymbol{\lambda}_j = (0, \ldots, 0, 1, -1, 1, -1, 0, \ldots, 0)^{\mathrm{T}}, \tag{A29}$$

where the nodes with nonzero entries are numbered along $\mathcal{P}$. Since any node not along $\mathcal{P}$ corresponds to a 0 in all of the $\boldsymbol{\lambda}_j$, we can consider just the induced subgraph of $\mathbf{U}$ restricted to $\mathcal{P}$—in other words, the submatrix of $\mathbf{U}$ restricted to the nodes along $\mathcal{P}$.

Inspection reveals that along $\mathcal{P}$, $\mathbf{U}$ for the toric code [Fig. 7(b)] is exactly like that of the GHZ state [Fig. 8(b)] except at the ends, where there is an extra edge connecting the two endpoints and self-loops of weight $2s^2 + s^{-2}$ instead of

$s^2 + s^{-2}$. Continuing with the example above (and omitting zeros),

$$\boldsymbol{\lambda}_j \boldsymbol{\lambda}_k^{\mathrm{T}} = \begin{pmatrix} & & & & \\ & 1 & -1 & 1 & -1 \\ & -1 & 1 & -1 & 1 \\ & 1 & -1 & 1 & -1 \\ & -1 & 1 & -1 & 1 \\ & & & & \end{pmatrix}, \tag{A30}$$

with the size of the blank padding on each side (representing zeros) left unspecified but determined by j and k.

The relevant part of $\mathbf{U}$ is *circulant* tridiagonal (nodes numbered according to $\mathcal{P}$) with all diagonal entries $2s^2 + s^{-2}$ (no difference at the ends because of periodicity) and all sub- and superdiagonal entries (continued in a circulant fashion) equal to s^2:

$$\mathbf{U} \mapsto \begin{pmatrix} a & s^2 & & & s^2 \\ s^2 & a & s^2 & & \\ & \ddots & \ddots & \ddots & \\ & & s^2 & a & s^2 \\ s^2 & & & s^2 & a \end{pmatrix}, \tag{A31}$$

where $a = 2s^2 + s^{-2}$, nodes are again ordered according to their appearance along $\mathcal{P}$, and $\mapsto$ indicates that only the relevant part of the full $\mathbf{U}$ is shown [cf. Eq. (A18)].

When $j = k$, the 4×4 block of ± 1 in Eq. (A30) is on the diagonal, and thus only the three innermost diagonals of that block matter when taking the entrywise inner product with $\mathbf{U}$. Therefore, for $w = 4$, $\langle \hat{M}_j^2 \rangle = \frac{1}{8}[4(2s^2 + s^{-2}) - 6s^2]$. When $j - k = \pm 1 \pmod n$, then the only entry that matters is the -1 in the upper right or bottom left of the block, and thus $\langle \hat{M}_j \hat{M}_{j\pm 1} \rangle = \frac{1}{8}(-s^2)$. Analogous results hold for other even values of w, but we will postpone the general formula until we consider the odd case.

When w is odd, the form of the number block in Eq. (A30) differs depending on whether $j - k$ is even or odd. This is because adjacent measurement operators have opposite sign configurations when adding up the individual $\hat{p}$ operators. Using $w = 3$ as an example,

$$\boldsymbol{\lambda}_j \boldsymbol{\lambda}_{j+\mathrm{even}}^{\mathrm{T}} = \begin{pmatrix} & & & \\ & 1 & -1 & 1 \\ & -1 & 1 & -1 \\ & 1 & -1 & 1 \\ & & & \end{pmatrix}, \tag{A32}$$

$$\boldsymbol{\lambda}_j \boldsymbol{\lambda}_{j+\mathrm{odd}}^{\mathrm{T}} = \begin{pmatrix} & & & \\ & -1 & 1 & -1 \\ & 1 & -1 & 1 \\ & -1 & 1 & -1 \\ & & & \end{pmatrix}, \tag{A33}$$

with the size of the blank padding on each side (again representing zeros) left unspecified but determined by j and k. Notice that, once again, for the same reasons as for even w, only the cases where $j = k$ or $j - k = \pm 1 \pmod n$ matter, and now the pattern for both even and odd w is clear (and the same in both cases):

$$\begin{aligned} \langle \hat{M}_j^2 \rangle &= \frac{1}{2w}[w(2s^2 + s^{-2}) - 2(w-1)s^2] \\ &= \frac{1}{2s^2} + \frac{s^2}{w}, \end{aligned} \tag{A34}$$

$$\langle \hat{M}_j \hat{M}_{j\pm 1} \rangle = \frac{-s^2}{2w}, \tag{A35}$$

where the ± 1 is mod n. These are the prebroadcast covariances of the players' measurement operators using a toric-code state. They also hold for the GHZ state with periodic boundary conditions, which is a special case of the torus.

The total measurement $\hat{M}$ has a matrix $\boldsymbol{\lambda}\boldsymbol{\lambda}^{\mathrm{T}}$ whose nonzero block is $nw \times nw$ and of the same form as Eq. (A27). Notice that in order to get the periodicity to match up, nw must be even. Examining the form of $\mathbf{U}$ in Eq. (A31), we see that we must add the diagonal of $\mathbf{U}$ and subtract its sub- and superdiagonals, including their circulant extensions (the entries in the corners). Therefore, we have the general result

$$(\Delta M)^2 = \langle \hat{M}^2 \rangle = \frac{1}{2nw}[nw(2s^2 + s^{-2}) - 2nw(s^2)] = \frac{1}{2s^2}, \tag{A36}$$

which holds for all n and w (with $nw \geqslant 4$ and even).

6. CV surface-code state with open boundaries

The calculations of sender anonymity and broadcast channel capacity assume a toric-code state, whose results were presented above. The optical implementation (Sec. VIII), however, proposes implementing the protocol using surface-code states with open boundaries instead. Here we show that this sort of resource also works.

The open-boundary surface-code state is shown in Fig. 9(b), where the top and bottom are "smooth" boundaries, and the left and right are "rough" boundaries, with terminology chosen by convention because of their visual representation in the graph. We can choose $\mathcal{P}$ to be any of the three horizontal lines of nodes in that graph that stretch all the way from the left boundary (rough) to the right boundary (also rough)—e.g., 3, 13, 23, 33. Alice will apply her displacements along $\tilde{\mathcal{P}}$, which could be, for instance, 11, 13, 15, or any of the vertical lines parallel to that one and that stretch all the way from the bottom boundary (smooth) to the top boundary (also smooth).

Notice that the self-loops at the rough boundaries [Fig. 9(b)] are like the endpoints of the CV GHZ state [Fig. 8(b)]. In fact, by the same logic as in the toric-code case above, the only part of $\mathbf{U}$ that will matter is the submatrix of the full $\mathbf{U}$ limited to the nodes along $\mathcal{P}$. This now has the exact same form as the $\mathbf{U}$ for the GHZ state, which is given in Eq. (A18). For n players, the surface-code state is divided into n vertical slices, each with arbitrary width w (with $nw \geqslant 4$ and even). Then, the matrix $\mathbf{U}$ becomes

$$\mathbf{U} \mapsto \begin{pmatrix} b & s^2 & & & \\ s^2 & a & s^2 & & \\ & \ddots & \ddots & \ddots & \\ & & s^2 & a & s^2 \\ & & & s^2 & b \end{pmatrix}, \tag{A37}$$

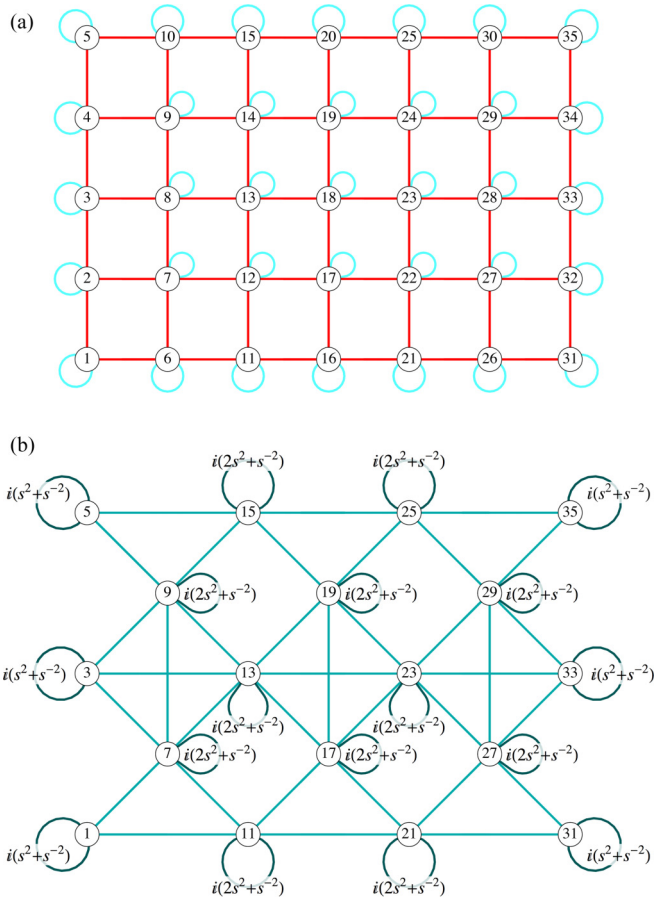

FIG. 9. Open-boundary CV cluster state and CV surface-code state. (a) CV cluster state with open boundaries. Red edges have weight 1, and cyan self-loops have weight is^{-2} [58]. (b) CV surface-code state with smooth boundaries on the top and bottom and with rough boundaries on the left and right. Unlabeled edges all have weight is^2. Starting from panel (a), the smooth boundaries are generated by measuring $\hat{p}$ on nodes 6, 16, 26, 10, 20, 30. The rough boundaries are generated by measuring $\hat{q}$ on nodes 2, 4, 32, 34. An alternating pattern of $\hat{p}$ and $\hat{q}$ measurements on all remaining even nodes completes the transition to the surface-code state. (The terms "smooth" and "rough" are chosen by convention to visually match the boundaries of the resulting graph.) Also notice that the three horizontal lines extending the full width of panel (b) have the same weights as the CV GHZ state from Fig. 8(b).

where $a = 2s^2 + s^{-2}$ and $b = s^2 + s^{-2}$, and $\mapsto$ again indicates that only the relevant part of $\mathbf{U}$ is displayed. Notice the two differences between this and Eq. (A31): In Eq. (A37), the first and last diagonal entries are different from the rest, and the isolated corner entries are missing.

Using the same arguments as above, we have the following variances within each player's slice and the interslice covariances:

$$\langle \hat{M}_1^2 \rangle = \langle \hat{M}_n^2 \rangle = \frac{1}{2w}[(w-1)(2s^2+s^{-2}) + (s^2+s^{-2}) - 2(w-1)s^2] = \frac{1}{2s^2} + \frac{s^2}{2w}, \tag{A38}$$

$$\langle \hat{M}_j^2 \rangle = \frac{1}{2w}[w(2s^2+s^{-2}) - 2(w-1)s^2] = \frac{1}{2s^2} + \frac{s^2}{w}, \tag{A39}$$

$$\langle \hat{M}_j \hat{M}_{j\pm1} \rangle = \frac{-s^2}{2w}, \tag{A40}$$

where $2 \leqslant j \leqslant n-1$. Notice that the ± 1 is no longer mod n. Also,

$$(\Delta M)^2 = \langle \hat{M}^2 \rangle = \frac{1}{2nw}[(nw-2)(2s^2+s^{-2}) + 2(s^2+s^{-2}) - 2(nw-1)s^2] = \frac{1}{2s^2}. \tag{A41}$$

In this case, the noise of the broadcast message is the same, $(\Delta M)^2 = \frac{1}{2s^2}$, which means the channel capacity is the same (Sec. IV). But now players 1 and n are more at risk of being discovered if one of them is the broadcaster. This is because the local noise in their measurement outcomes is less than that of the other players, and it is this local noise that hides the fact that any individual player has broadcast a message (Sec. V).

One might be tempted to think that making the end slices (1 and n) narrower, with a width of $\frac{w}{2}$ instead of w, could make the local noise the same for all players. This is true—but misleading. The reason for this is that if player 1 or n wanted to broadcast a message r, her measurement outcome would be displaced further than would that of players $2, \ldots, n-1$ if one of them instead had broadcast the same message—in fact, further by a factor of $\sqrt{2}$ [see Eq. (25)]. This means that the variance of that displacement is twice what it would be had she used a full w-width slice. This effectively nullifies the advantage of increased local noise in the narrower slice. Either way, the local signal-to-noise ratio (which governs the risk of broadcaster discovery) is approximately twice what it would be for any of the other players wishing to broadcast the same message. Thus, there is no advantage to using narrower slices at the ends.

APPENDIX B: WEDGE WIDTH IN FIGURE 5

The results summarized in Fig. 2 assume that the players have received wedges of width $w = 6$. Here we justify this choice.

Assume that in addition to the dissipative error mitigation proposed in the main text, one can also perform measurements of the number of excitations in the nullifiers. A detected excitation indicates an error in the code (a jump out of the code space) in the neighborhood of that nullifier. We then logically tag that location as a part of the code to be avoided—effectively declaring the modes in that neighborhood lost completely. This conservative choice allows us to steer clear of detected errors altogether.

For rates of lost (i.e., error-tagged) nodes below the toric-code error tolerance rate of 50% (error per mode $p_{\text{err}} = \frac{1}{2}$ per physical operation), as derived from the percolation threshold for a square lattice [64], paths can be found that connect the lattice along homologically nontrivial loops. Communication between players restricts the allowable density of errors and

defines a lower bound for the width of each wedge. For occupation probability p below the percolation threshold p_c, the probability that there is a cluster of radius r in the percolation model is given by $p_{\text{cluster}}(r) \approx e^{-r|p-p_c|^\nu}$ where ν is the critical exponent [65]. For bond percolation on a square lattice in two dimensions, $p_c = \frac{1}{2}$ and $\nu = \frac{4}{3}$, so the probability the protocol fails due to these errors is

$$p_{\text{fail}} \approx e^{-\frac{w}{2}|p_{\text{err}}-\frac{1}{2}|^{4/3}}. \tag{B1}$$

Hence, for a target p_{fail}, we have

$$w \geqslant \frac{2\log\left(p_{\text{fail}}^{-1}\right)}{\left|p_{\text{err}}-\frac{1}{2}\right|^{4/3}}. \tag{B2}$$

Assume errors can be monitored, for instance using the protocol described in the main text. Then, if one of the players measures a percolated cluster of errors on her wedge, she can announce an abort warning to the others. The whole protocol can then be retried, and the probability of failure after k attempts is p_{fail}^k. Say we fix $p_{\text{fail}} = 1/e$, implying

$$w \geqslant \frac{2}{\left|p_{\text{err}}-\frac{1}{2}\right|^{4/3}}. \tag{B3}$$

Then, assuming an error rate $p_{\text{err}} < 0.06$, a wedge width of $w = 6$ will suffice. This percolation argument also assumes a circumference of the wedge around the same size.

APPENDIX C: MATHEMATICAL RESULTS

Here we provide mathematical results that are used in Secs. IV and V.

1. Gaussian distributions: Notation and entropic properties

We adopt the following notation for a random variable X with instantiations $x \in \mathbb{R}$ distributed according to a Gaussian (normal) distribution with mean $\langle X\rangle = \mu$ and variance $\text{var}(X) = \langle (X-\mu)^2\rangle = \sigma^2$:

$$X \sim N_{\mu,\sigma^2}(x) = \frac{1}{\sqrt{2\pi\sigma^2}}\exp\left[-\frac{(x-\mu)^2}{2\sigma^2}\right]. \tag{C1}$$

This can easily be extended to a random column vector $\mathbf{X}$ with instantiations $\mathbf{x} \in \mathbb{R}^n$ distributed according to a multivariate Gaussian with mean $\langle \mathbf{X}\rangle = \boldsymbol{\mu}$ and covariance matrix $\text{cov}(\mathbf{X}) = \langle (\mathbf{X}-\boldsymbol{\mu})(\mathbf{X}-\boldsymbol{\mu})^{\mathrm{T}}\rangle = \boldsymbol{\Sigma} > 0$:

$$\begin{aligned}\mathbf{X} &\sim N_{\boldsymbol{\mu},\boldsymbol{\Sigma}}(\mathbf{x})\\ &= \frac{1}{\sqrt{\det(2\pi\boldsymbol{\Sigma})}}\exp\left[-\frac{1}{2}(\mathbf{x}-\boldsymbol{\mu})^{\mathrm{T}}\boldsymbol{\Sigma}^{-1}(\mathbf{x}-\boldsymbol{\mu})\right].\end{aligned} \tag{C2}$$

The entropy of the univariate Gaussian is

$$H(X) = \langle -\log N_{\mu,\sigma^2}(X)\rangle = \tfrac{1}{2}\log(2\pi e\sigma^2). \tag{C3}$$

Note that we leave the base unspecified. Therefore, all entropies in this document are expressed in bits if the log based is 2, in nats if the log base is e, etc. Its multivariate generalization is

$$H(\mathbf{X}) = \langle -\log N_{\boldsymbol{\mu},\boldsymbol{\Sigma}}(\mathbf{X})\rangle = \tfrac{1}{2}\log\det(2\pi e\boldsymbol{\Sigma}). \tag{C4}$$

For any random vector $\mathbf{Y}$—not necessarily Gaussian—with mean $\boldsymbol{\mu}$ and covariance $\boldsymbol{\Sigma}$, its entropy is bounded from above by the entropy of a Gaussian-distributed random vector with the same covariance. In other words,

$$H(\mathbf{Y}) \leqslant \tfrac{1}{2}\log\det(2\pi e\boldsymbol{\Sigma}) = H(\mathbf{X}). \tag{C5}$$

2. Special cases of symmetric, tridiagonal, Toeplitz/circulant matrices

Consider the two $n \times n$ matrices

$$\mathbf{T}_n(x) := \begin{pmatrix} x & 1 & & & & & \\ 1 & x & 1 & & & & \\ & 1 & x & 1 & & & \\ & & \ddots & \ddots & \ddots & & \\ & & & 1 & x & 1 & \\ & & & & 1 & x & 1 \\ & & & & & 1 & x \end{pmatrix} \tag{C6}$$

and

$$\mathbf{C}_n(x) := \begin{pmatrix} x & 1 & & & & & 1 \\ 1 & x & 1 & & & & \\ & 1 & x & 1 & & & \\ & & \ddots & \ddots & \ddots & & \\ & & & 1 & x & 1 & \\ & & & & 1 & x & 1 \\ 1 & & & & & 1 & x \end{pmatrix}, \tag{C7}$$

with constant diagonal bands understood and missing entries taken to be 0. The notation is chosen because $\mathbf{T}_n(x)$ is a Toeplitz matrix and $\mathbf{C}_n(x)$ is its circulant counterpart. These matrices are uniquely defined for $n \geqslant 3$. We can complete the definition for all $n \in \mathbb{N}_+$ by also defining

$$\mathbf{T}_1(x) = \mathbf{C}_1(x) := (x), \tag{C8}$$

$$\mathbf{T}_2(x) = \mathbf{C}_2(x) := \begin{pmatrix} x & 1 \\ 1 & x \end{pmatrix}. \tag{C9}$$

Now let us consider their determinants.

Define $t_n(x) := \det \mathbf{T}_n(x)$. Using the cofactor expansion of the determinant, we see that the following recurrence relation holds for $n \geqslant 3$ [66,67]:

$$t_n(x) = xt_{n-1}(x) - t_{n-2}(x). \tag{C10}$$

Since $t_2(x) = x^2 - 1$ and $t_1(x) = x$ by direct calculation, we see that this recurrence relation also holds for $n = 2$ if we choose $t_0(x) := 1$. These are exactly the recurrence relation and initial conditions for the Chebyshev polynomials of the second kind $U_n(\frac{x}{2})$. Therefore,

$$\det \mathbf{T}_n(x) = t_n(x) = U_n\left(\frac{x}{2}\right). \tag{C11}$$

This result also agrees with the literature [68–71] after applying properties of Chebyshev polynomials.

Define $c_n(x) := \det \mathbf{C}_n(x)$. A cofactor expansion for $n \geqslant 3$ relates this to the result for the Toeplitz case:

$$c_n(x) = xt_{n-1}(x) - 2[t_{n-2}(x) + (-1)^n]. \tag{C12}$$

Plugging in Eq. (C11) and using properties of Chebyshev polynomials gives

$$c_n(x) = 2(-1)^n\left[T_n\left(-\frac{x}{2}\right) - 1\right], \tag{C13}$$

where T_n is the nth-order Chebyshev polynomial of the first kind, valid for $n \geqslant 3$. Note that $c_2(x) = t_2(x)$ and $c_1(x) = t_1(x)$. Therefore,

$$\det \mathbf{C}_n(x) = c_n(x) = \begin{cases} U_n\left(\frac{x}{2}\right) & \text{if } n \in \{1,2\}, \\ 2(-1)^n\left[T_n\left(-\frac{x}{2}\right) - 1\right] & \text{if } n \geqslant 3. \end{cases} \tag{C14}$$

Now consider a perturbed version of the circulant matrix above:

$$\mathbf{C}_n(x,a) := \begin{pmatrix} x+a & 1 & & & & & 1 \\ 1 & x & 1 & & & & \\ & 1 & x & 1 & & & \\ & & \ddots & \ddots & \ddots & & \\ & & & 1 & x & 1 & \\ & & & & 1 & x & 1 \\ 1 & & & & & 1 & x \end{pmatrix}. \tag{C15}$$

Cofactor evaluation of its determinant gives

$$\det \mathbf{C}_n(x,a) = \det \mathbf{C}_n(x) + a \det \mathbf{T}_{n-1}(x). \tag{C16}$$

Specializing to $n \geqslant 3$ evaluates this to

$$\begin{aligned} \det \mathbf{C}_n(x,a) &= 2(-1)^n\left[T_n\left(-\frac{x}{2}\right) - 1\right] + aU_{n-1}\left(\frac{x}{2}\right) \\ &= 2(-1)^n\left(1 + \frac{a}{n}\frac{\partial}{\partial x}\right)\left[T_n\left(-\frac{x}{2}\right) - 1\right]. \end{aligned} \tag{C17}$$

Notice that this means

$$\det \mathbf{C}_n(x,a) = \left(1 + \frac{a}{n}\frac{\partial}{\partial x}\right) \det \mathbf{C}_n(x), \tag{C18}$$

which can be also be verified using Jacobi's identity. Direct evaluation for $n = 1$ and $n = 2$ show that Eq. (C18) is also valid for those cases and therefore valid for all $n \in \mathbb{N}_+$.

APPENDIX D: DISSIPATIVE GAUSSIAN DYNAMICS

For N modes undergoing Gaussian dynamics, the master equation describes the evolution of the means and covariance matrix $\mathbf{\Sigma}$. Defining a column vector of stacked quadrature operators

$$\hat{\mathbf{r}} := \begin{pmatrix} \hat{\mathbf{q}} \\ \hat{\mathbf{p}} \end{pmatrix}, \tag{D1}$$

the commutation relations can be expressed as

$$[\hat{\mathbf{r}}, \hat{\mathbf{r}}^{\mathrm{T}}] = \hat{\mathbf{r}}\hat{\mathbf{r}}^{\mathrm{T}} - (\hat{\mathbf{r}}\hat{\mathbf{r}}^{\mathrm{T}})^{\mathrm{T}} = i\mathbf{\Omega}, \tag{D2}$$

where $^{\mathrm{T}}$ indicates matrix transpose (see Ref. [58] for more details on this notation). The matrix $\mathbf{\Omega}$ is known as the *symplectic form*:

$$\mathbf{\Omega} = \begin{pmatrix} \mathbf{0} & \mathbf{I} \\ -\mathbf{I} & \mathbf{0} \end{pmatrix}, \tag{D3}$$

where $\mathbf{I}$ is the $N \times N$ identity matrix. For dissipative evolution given by a Markov master equation, Gaussianity is preserved under two conditions. First, the Hamiltonian must have the quadratic form

$$\hat{H} = \tfrac{1}{2}\hat{\mathbf{r}}^{\mathrm{T}}\mathbf{G}\hat{\mathbf{r}}, \tag{D4}$$

expressed in terms of the symmetric, real matrix $\mathbf{G} \in \mathbb{R}^{2N\times 2N}$. Second, the jump operators that describe coupling to M baths must be linear in the mode operators. The jump operator that couples to bath k therefore must have the form

$$\hat{L}_k = \sum_{j=1}^{N}(Q_{kj}\hat{q}_j + P_{kj}\hat{p}_j). \tag{D5}$$

We collect all M of these jump operators into the vector of operators denoted

$$\hat{\mathbf{L}} = \mathbf{C}\hat{\mathbf{r}}, \tag{D6}$$

where we have defined $\mathbf{C} := (\mathbf{Q} \quad \mathbf{P}) \in \mathbb{C}^{M\times 2N}$, and the matrices $\mathbf{Q}$ and $\mathbf{P}$ (which contain the cooling rates) are comprised of the coefficients in Eq. (D5). Then, the symmetrized covariance matrix obeys the following equations of motion:

$$\frac{d}{dt}\mathbf{\Sigma} = \mathbf{A}\mathbf{\Sigma} + \mathbf{\Sigma}\mathbf{A}^{\mathrm{T}} + \mathbf{B}, \tag{D7}$$

with matrices

$$\mathbf{A} := \mathbf{\Omega}[\mathbf{G} + \mathrm{Im}(\mathbf{C}^{\mathrm{H}}\mathbf{C})], \tag{D8}$$

$$\mathbf{B} := \mathbf{\Omega}\,\mathrm{Re}(\mathbf{C}^{\mathrm{H}}\mathbf{C})\mathbf{\Omega}^{\mathrm{T}}. \tag{D9}$$

The superscript $^{\mathrm{H}}$ indicates conjugate transpose of a matrix (to distinguish it from the Hermitian adjoint of an individual operator; see Ref. [58]).

For the master equation in Eq. (69), we have $\mathbf{G} = \mathbf{0}$ and

$$\mathbf{C}^{\mathrm{H}}\mathbf{C} = \begin{pmatrix} \mathbf{R}_p & i\mathbf{T} \\ -i\mathbf{T} & \mathbf{R}_q \end{pmatrix}, \tag{D10}$$

where $\mathbf{T}$, $\mathbf{R}_q$, and $\mathbf{R}_p$ are symmetric, real matrices. The $\mathbf{A}$ and $\mathbf{B}$ matrices are block diagonal:

$$\mathbf{A} = -\begin{pmatrix} \mathbf{T} & \mathbf{0} \\ \mathbf{0} & \mathbf{T} \end{pmatrix}, \quad \mathbf{B} = \begin{pmatrix} \mathbf{R}_q & \mathbf{0} \\ \mathbf{0} & \mathbf{R}_p \end{pmatrix}. \tag{D11}$$

The matrix blocks that comprise $\mathbf{A}$ and $\mathbf{B}$ each have a portion corresponding to the CV toric-code cooling map and a diagonal portion corresponding to the local loss,

$$\mathbf{T} = \mathbf{T}_{\mathrm{TC}} + \frac{\gamma_{\mathrm{loss}}}{2}\mathbf{I}, \tag{D12}$$

$$\mathbf{R}_i = \mathbf{R}_{\mathrm{TC},i} + \frac{\gamma_{\mathrm{loss}}}{2}\mathbf{I}, \tag{D13}$$

where $i \in \{q,p\}$.

Because of the block structure of $\mathbf{A}$ and $\mathbf{B}$, the matrix blocks of the covariance matrix that describe quadrature correlations,

$$\mathbf{\Sigma} := \begin{pmatrix} \mathbf{\Sigma}_{qq} & \mathbf{\Sigma}_{qp} \\ \mathbf{\Sigma}_{pq} & \mathbf{\Sigma}_{pp} \end{pmatrix}, \tag{D14}$$

evolve independently. Assuming no qp correlations, $\mathbf{\Sigma}_{qp} = \mathbf{\Sigma}_{pq} = \mathbf{0}$, and the diagonal matrix blocks evolve according to

$$\frac{d}{dt}\mathbf{\Sigma}_{qq} = -\mathbf{T}\mathbf{\Sigma}_{qq} - \mathbf{\Sigma}_{qq}\mathbf{T} + \mathbf{R}_q, \tag{D15a}$$

$$\frac{d}{dt}\mathbf{\Sigma}_{pp} = -\mathbf{T}\mathbf{\Sigma}_{pp} - \mathbf{\Sigma}_{pp}\mathbf{T} + \mathbf{R}_p. \tag{D15b}$$

These equations were solved numerically with initial state $|\mathrm{GS}_{\mathrm{vac}}\rangle$ [from Eq. (12)] to produce the results presented in Fig. 4. There are two facts to note about $|\mathrm{GS}_{\mathrm{vac}}\rangle$. First, it is a Gaussian state since it is the ground state of a quadratic

Hamiltonian

$$\hat{H}_{\mathrm{SC}} = \sum_{i \in \mathcal{V} \cup \mathcal{F}} \hat{\eta}_i^\dagger \hat{\eta}_i + \hat{a}_1^\dagger \hat{a}_1 + \hat{a}_2^\dagger \hat{a}_2, \tag{D16}$$

where $\hat{a}_1$ and $\hat{a}_2$ are canonical annihilation operators on the distributed logical modes. Second, $|\mathrm{GS}_{\mathrm{vac}}\rangle$ is an $\mathcal{H}$-graph state [58] and has no qp correlations.

The matrix-block evolution can be solved analytically for the covariance matrix corresponding to the steady-state density matrix $\hat{\rho}_{\mathrm{ss}}$:

$$\mathbf{\Sigma}_{qq}(t \to \infty) = \tfrac{1}{2}\mathbf{T}^{-1}\mathbf{R}_q, \tag{D17a}$$

$$\mathbf{\Sigma}_{pp}(t \to \infty) = \tfrac{1}{2}\mathbf{T}^{-1}\mathbf{R}_p. \tag{D17b}$$

In the absence of cooling ($\gamma_{\mathrm{cool}} = 0$), the steady state is vacuum. In the opposite regime where there is no loss ($\gamma_{\mathrm{loss}} = 0$), the steady state is a CV toric-code state, $\hat{\rho}_{\mathrm{ss}} = |\boldsymbol{\eta}\rangle\langle\boldsymbol{\eta}|_{\mathrm{null}} \otimes \hat{\rho}_{\mathcal{L}}$, which depends on the initial state and is in general mixed. When the initial state is the local vacuum, this yields the toric-code vacuum state given by Eq. (12), $\hat{\rho}_{\mathrm{ss}} = |\mathrm{GS}_{\mathrm{vac}}\rangle\langle\mathrm{GS}_{\mathrm{vac}}|$. In the general case both loss and cooling are present, and the steady state is neither pure nor is it a CV toric-code state ($\mathrm{tr}[\hat{\eta}_i^\dagger \hat{\eta}_i \hat{\rho}_{\mathrm{ss}}] \neq 0$ for some or all of the nullifiers). However, for cooling that greatly outweighs loss ($\gamma_{\mathrm{cool}}/\gamma_{\mathrm{loss}} \gg 1$), the steady state can be close to the CV toric-code vacuum, $|\mathrm{GS}_{\mathrm{vac}}\rangle$, as shown in Fig. 4(a).

[1] M. Movahedi, J. Saia, and M. Zamani, Secure anonymous broadcast, arXiv:1405.5326v1.

[2] F. Stajano and R. Anderson, The cocaine auction protocol: On the power of anonymous broadcast, in *Information Hiding* (Springer, Berlin, 2000), pp. 434–447.

[3] T. Ruffing, P. Moreno-Sanchez, and A. Kate, P2P Mixing and Unlinkable Bitcoin Transactions, Cryptology ePrint Archive, Report 2016/824, https://eprint.iacr.org/2016/824.

[4] D. Chaum, The dining cryptographers problem: Unconditional sender and recipient untraceability, J. Cryptol. **1**, 65 (1988).

[5] A. Broadbent and A. Tapp, Information-theoretic security without an honest majority, in *Proceedings of ASIACRYPT 2007* (Springer, Berlin, 2007), pp. 410–426.

[6] A. Broadbent, S. Jeffrey, and A. Tapp, Exact, efficient, and information-theoretically secure voting with an arbitrary number of cheaters, arXiv:1011.5242.

[7] P. O. Boykin, Information security and quantum mechanics: Security of quantum protocols, arXiv:quant-ph/0210194.

[8] M. Christandl and S. Wehner, Quantum anonymous transmissions, in *Proceedings of ASIACRYPT 2005, LNCS 3788* (Springer, Berlin, 2005), pp. 217–235.

[9] G. Brassard, A. Broadbent, J. Fitzsimons, S. Gambs, and A. Tapp, Anonymous quantum communication, in *Proceedings of ASIACRYPT, 2007* (Springer, Berlin, 2007), pp. 460–473.

[10] X.-Q. Cai and H.-F. Niu, Quantum private communication with an anonymous sender, Int. J. Theor. Phys. **52**, 411 (2013).

[11] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2000).

[12] A. Y. Kitaev, Fault-tolerant quantum computation by anyons, Ann. Phys. **303**, 2 (2003).

[13] J. K. Pachos, *Introduction to Topological Quantum Computation* (Cambridge University Press, Cambridge, UK, 2012).

[14] R. Barends, J. Kelly, A. Megrant, A. Veitia, D. Sank, E. Jeffrey, T. C. White, J. Mutus, A. G. Fowler, B. Campbell *et al.*, Superconducting quantum circuits at the surface code threshold for fault tolerance, Nature (London) **508**, 500 (2014).

[15] M. Suchara, J. Kubiatowicz, A. Faruque, F. Chong, C. Lai, and G. Paz-Silva, in *Proceedings of the 31st IEEE International Conference on Computer Design* (IEEE, Asheville, North Carolina, 2013), p. 419.

[16] 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).

[17] J. Pachos, *Introduction to Topological Quantum Computation* (Cambridge University Press, Cambridge, UK, 2012).

[18] A. Hamma, R. Ionicioiu, and P. Zanardi, Bipartite entanglement and entropic boundary law in lattice spin systems, Phys. Rev. A **71**, 022315 (2005).

[19] S. S. Bullock and G. K. Brennen, Qudit surface codes and gauge theory with finite cyclic groups, J. Phys. A: Math. Theor. **40**, 3481 (2007).

[20] A. G. Fowler, A. C. Whiteside, and L. C. L. Hollenberg, Towards practical classical processing for the surface code: Timing analysis, Phys. Rev. A **86**, 042313 (2012).

[21] H. Anwar, Towards fault-tolerant quantum computation with higher-dimensional systems, Ph.D. thesis, University College London, London, 2014 (unpublished).

[22] G. K. Brennen, D. Song, and C. Williams, Quantum-computer architecture using nonlocal interactions, Phys. Rev. A **67**, 050302(R) (2003).

[23] J. Zhang, C. Xie, K. Peng, and P. van Loock, Anyon statistics with continuous variables, Phys. Rev. A **78**, 052121 (2008).

[24] D. F. Walls and G. J. Milburn, *Quantum Optics*, 2nd ed. (Springer, Berlin, 2008).

[25] C. E. Shannon, Communication in the presence of noise, Proc. IRE **37**, 10 (1949).

[26] C. E. Shannon, Probability of error for optimal codes in a Gaussian channel, Bell Syst. Tech. J. **38**, 611 (1959).

[27] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (John Wiley & Sons, New York, 2012).

[28] E. T. Jaynes, *Probability Theory: The Logic of Science* (Cambridge University Press, Cambridge, UK, 2003).

[29] R. Urbanke and B. Rimoldi, Lattice codes can achieve capacity on the AWGN channel, IEEE Trans. Inform. Theory **44**, 273 (1998).

[30] S. Berens, Conditional Rényi entropy, Master's thesis, Leiden University, 2013 (unpublished).

[31] A. Genz and F. Bretz, *Computation of Multivariate Normal and t Probabilities*, Lecture Notes in Statistics Vol. 195 (Springer-Verlag, Berlin, 2009).

[32] S. Diehl, A. Micheli, A. Kantian, B. Kraus, H. P. Büchler, and P. Zoller, Quantum states and phases in driven open quantum systems with cold atoms, Nat. Phys. **4**, 878 (2008).

[33] C. W. Gardiner and P. Zoller, *Quantum Noise*, 3rd ed. (Springer, Berlin, 2004).

[34] R. Jozsa, Fidelity for mixed quantum states, J. Mod. Opt. **41**, 2315 (1994).

[35] G. Spedalieri, C. Weedbrook, and S. Pirandola, A limit formula for the quantum fidelity, J. Phys. A **46**, 025304 (2013).
[36] P. Wang, M. Chen, N. C. Menicucci, and O. Pfister, Weaving quantum optical frequency combs into continuous-variable hypercubic cluster states, Phys. Rev. A **90**, 032325 (2014).
[37] M. Chen, N. C. Menicucci, and O. Pfister, Experimental Realization of Multipartite Entanglement of 60 Modes of a Quantum Optical Frequency Comb, Phys. Rev. Lett. **112**, 120505 (2014).
[38] N. C. Menicucci, Temporal-mode continuous-variable cluster states using linear optics, Phys. Rev. A **83**, 062314 (2011).
[39] S. Yokoyama, R. Ukai, S. C. Armstrong, C. Sornphiphatphong, T. Kaji, S. Suzuki, J. Yoshikawa, H. Yonezawa, N. C. Menicucci, and A. Furusawa, Ultra-large-scale continuous-variable cluster states multiplexed in the time domain, Nat. Photon. **7**, 982 (2013).
[40] T. Eberle, S. Steinlechner, J. Bauchrowitz, V. Händchen, H. Vahlbruch, M. Mehmet, H. Müller-Ebhardt, and R. Schnabel, Quantum Enhancement of the Zero-Area Sagnac Interferometer Topology for Gravitational Wave Detection, Phys. Rev. Lett. **104**, 251102 (2010).
[41] M. Mehmet, S. Ast, T. Eberle, S. Steinlechner, H. Vahlbruch, and R. Schnabel, Squeezed light at 1550 nm with a quantum noise reduction of 12.3 dB, Opt. Express **19**, 25763 (2011).
[42] G. A. Paz-Silva, S. Rebić, J. Twamley, and T. Duty, Perfect Mirror Transport Protocol with Higher Dimensional Quantum Chains, Phys. Rev. Lett. **102**, 020503 (2009).
[43] B. Yurke, P. G. Kaminsky, R. E. Miller, E. A. Whittaker, A. D. Smith, A. H. Silver, and R. W. Simon, Observation of 4.2-K Equilibrium-Noise Squeezing Via a Josephson-Parametric Amplifier, Phys. Rev. Lett. **60**, 764 (1988).
[44] M. A. Castellanos-Beltran, K. D. Irwin, G. C. Hilton, L. R. Vale, and K. W. Lehnert, Amplification and squeezing of quantum noise with a tunable Josephson metamaterial, Nat. Phys. **4**, 929 (2008).
[45] E. Flurin, N. Roch, F. Mallet, M. H. Devoret, and B. Huard, Generating Entangled Microwave Radiation Over Two Transmission Lines, Phys. Rev. Lett. **109**, 183901 (2012).
[46] N. Bergeal, F. Schackert, L. Frunzio, and M. H. Devoret, Two-Mode Correlation of Microwave Quantum Noise Generated by Parametric Down-Conversion, Phys. Rev. Lett. **108**, 123902 (2012).
[47] C. Eichler, D. Bozyigit, C. Lang, M. Baur, L. Steffen, J. M. Fink, S. Filipp, and A. Wallraff, Observation of Two-Mode Squeezing in the Microwave Frequency Domain, Phys. Rev. Lett. **107**, 113601 (2011).
[48] C. M. Wilson, G. Johansson, A. Pourkabirian, M. Simoen, J. R. Johansson, T. Duty, F. Nori, and P. Delsing, Observation of the dynamical Casimir effect in a superconducting circuit, Nature (London) **479**, 376 (2011).
[49] M. H. Devoret, S. Girvin, and R. Schoelkopf, Circuit-QED: How strong can the coupling between a Josephson junction atom and a transmission line resonator be?, Ann. Phys. **16**, 767 (2007).
[50] S. Ashhab and F. Nori, Qubit-oscillator systems in the ultrastrong-coupling regime and their potential for preparing nonclassical states, Phys. Rev. A **81**, 042311 (2010).
[51] M. S. Allman, J. D. Whittaker, M. Castellanos-Beltran, K. Cicak, F. da Silva, M. P. DeFeo, F. Lecocq, A. Sirois, J. D. Teufel, J. Aumentado, and R. W. Simmonds, Tunable Resonant and Nonresonant Interactions Between a Phase Qubit and LC Resonator, Phys. Rev. Lett. **112**, 123601 (2014).
[52] K. Moon and S. M. Girvin, Theory of Microwave Parametric Down-Conversion and Squeezing using Circuit QED, Phys. Rev. Lett. **95**, 140504 (2005).
[53] A. M. Zagoskin, E. Il'ichev, M. W. McCutcheon, J. F. Young, and F. Nori, Controlled Generation of Squeezed States of Microwave Radiation in a Superconducting Resonant Circuit, Phys. Rev. Lett. **101**, 253602 (2008).
[54] W. Yi Huo and G. Lu Long, Entanglement and squeezing in solid-state circuits, New J. Phys. **10**, 013026 (2008).
[55] P.-B. Li and F.-L. Li, Engineering squeezed states of microwave radiation with circuit quantum electrodynamics, Phys. Rev. A **83**, 035807 (2011).
[56] A. Grimsmo and A. Blais, Squeezing and quantum state engineering with Josephson travelling wave amplifiers, npj Quantum Inf. **3**, 20 (2017).
[57] J. Yoshikawa, S. Yokoyama, T. Kaji, C. Sornphiphatphong, Y. Shiozawa, K. Makino, and A. Furasawa, Generation of one-million-mode continuous-variable cluster state by unlimited time-domain multiplexing, APL Photon. **1**, 060801 (2016).
[58] N. C. Menicucci, S. T. Flammia, and P. van Loock, Graphical calculus for Gaussian pure states, Phys. Rev. A **83**, 042335 (2011).
[59] N. C. Menicucci, S. T. Flammia, and O. Pfister, One-Way Quantum Computing in the Optical Frequency Comb, Phys. Rev. Lett. **101**, 130501 (2008).
[60] S. T. Flammia, N. C. Menicucci, and O. Pfister, The optical frequency comb as a one-way quantum computer, J. Phys. B **42**, 114009 (2009).
[61] R. N. Alexander, S. C. Armstrong, R. Ukai, and N. C. Menicucci, Noise analysis of single-mode Gaussian operations using continuous-variable cluster states, Phys. Rev. A **90**, 062324 (2014).
[62] H. Vahlbruch, M. Mehmet, K. Danzmann, and R. Schnabel, Detection of 15 dB Squeezed States of Light and Their Application for the Absolute Calibration of Photoelectric Quantum Efficiency, Phys. Rev. Lett. **117**, 110801 (2016).
[63] L. Jiang, G. He, D. Nie, J. Xiong, and G. Zeng, Quantum anonymous voting for continuous variables, Phys. Rev. A **85**, 042309 (2012).
[64] T. M. Stace, S. D. Barrett, and A. C. Doherty, Thresholds for Topological Codes in the Presence of Loss, Phys. Rev. Lett. **102**, 200501 (2009).
[65] G. Grimmett, *Percolation* (Springer Science & Business Media, Berlin, 1999).
[66] J. Borowska and L. Łacińska, Recurrence form for determinant of a heptadiagonal symmetric Toeplitz matrix, J. Appl. Math. Comput. Mech. **13**, 19 (2014).
[67] Z. Cinkir, A fast elementary algorithm for computing the determinant of Toeplitz matrices, J. Comput. Appl. Math. **255**, 353 (2014).
[68] G. Y. Hu and R. F. O'Connell, Analytical inversion of symmetric tridiagonal matrices, J. Phys. A: Math. Gen. **29**, 1511 (1996).
[69] M. Elouafi, On a relationship between Chebyshev polynomials and Toeplitz determinants, Appl. Math. Comput. **229**, 27 (2014).
[70] R. Álvarez-Nodarse, J. Petronilho, and N. R. Quintero, Spectral properties of certain tridiagonal matrices, Linear Algebra Appl. **436**, 682 (2012).
[71] C. M. Da Fonseca and J. Petronilho, Explicit inverse of a tridiagonal k Toeplitz matrix, Numer. Math. **100**, 457 (2005).