Random coding for sharing bosonic quantum secrets

Francesco Arzani, Giulia Ferrini, Frédéric Grosshans, Damian Markham

Random coding for sharing bosonic quantum secrets

Francesco Arzani,[1,2,*] Giulia Ferrini,[3] Frédéric Grosshans,[4,2,5] and Damian Markham[2,5]

[1] *Université de Lorraine, CNRS, Inria, LORIA, F 54000 Nancy, France*
[2] *Sorbonne Université, CNRS, Laboratoire d'Informatique de Paris 6, F-75005 Paris, France*
[3] *Department of Microtechnology and Nanoscience (MC2), Chalmers University of Technology, SE-412 96 Gothenburg, Sweden*
[4] *Laboratoire Aimé Cotton, CNRS, Univ. Paris-Sud, ENS Cachan, Univ. Paris Saclay, 91405 Orsay Cedex, France*
[5] *Paris Center for Quantum Computing, CNRS FR3640, Paris, France*

(Dated: August 6, 2019)

We consider a protocol for sharing quantum states using continuous variable systems. Specifically we introduce an encoding procedure where bosonic modes in arbitrary secret states are mixed with several ancillary squeezed modes through a passive interferometer. We derive simple conditions on the interferometer for this encoding to define a secret sharing protocol and we prove that they are satisfied by almost any interferometer. This implies that, if the interferometer is chosen uniformly at random, the probability that it may not be used to implement a quantum secret sharing protocol is zero. Furthermore, we show that the decoding operation can be obtained and implemented efficiently with a Gaussian unitary using a number of single-mode squeezers that is at most twice the number of modes of the secret, regardless of the number of players. We benchmark the quality of the reconstructed state by computing the fidelity with the secret state as a function of the input squeezing.

I. INTRODUCTION

Quantum systems are notoriously fragile: small losses or weak interactions with the outside world usually destroy quantum coherence. Since quantum information cannot be copied [1], any leakage of information leads to its destruction in the original system. To fully retrieve it, one usually needs full control over the environment. This loss of coherence is at the heart of quantum information, whether we want to fight it [2–4] or impose it on an adversary [5–7], but it plays an important role in a broader area of physics, including thermodynamics [8, 9], quantum control [10, 11], and black hole physics [12–16].

Among the strategies devised to try and overcome this fragility are quantum error correcting (QEC) codes [17, 18] and quantum secret sharing (QSS) schemes [19–21].

In QSS schemes, a *dealer* delocalizes the information between several players, so that authorized subsets of them (*access parties*) can fully reconstruct the original information without the shares of the other players. Unauthorized sets (*adversaries*) on the other hand get in principle no information about the secret. QSS schemes are equivalent to erasure correcting codes [19], protecting against loss of part of the system. As well as protecting information, they have many applications in quantum information, such as secure multiparty computation [22]. Most QSS and QEC schemes [17, 20, 21] are highly structured. However, random codes have been proven to optimally protect the state of a set of qubits from erasure errors [18]. Furthermore, their randomness makes them a natural model in a variety of physical scenarios where information is lost.

Most of these results are for two-dimensional, qubit encodings. Alternative to qubits, information can be encoded in the state of infinite-dimensional quantum systems, known as continuous-variable (CV) systems. CV systems are of great practical importance in quantum technologies [23]: the possibility to experimentally generate entanglement in a deterministic fashion makes them interesting candidates for the realization of quantum communication and computation protocols. Several CV generalizations of QSS [24–27] and erasure-correcting codes [28, 29] have been proposed, and some have been experimentally demonstrated [30–32]. Each of these schemes, however, requires encoding the secret in carefully chosen states. No CV random code has been proposed to date. This gap poses serious limitations to the experimental realization of CV-QSS. For example, unless the experimental setup is specifically tailored for the task, CV-QSS could not be carried out, or experimental imperfections might hinder its implementation. As in the qubit case, one may also expect applications of random coding beyond QSS and quantum information [12–16].

In this work, we fill this gap by introducing a form of random coding for CV. Namely, we show that QSS can be implemented in bosonic systems mixing a secret state with squeezed states, the workhorse of CV quantum information [33, 34], through *almost any* energy preserving transformation. The latter correspond to passive interferometers in the optical setting. Our approach also generalizes earlier proposals by allowing the secret to be an arbitrary multimode state, as long as enough players are considered. We show that for almost any passive transformation there exists a decoding scheme, that each authorized set can construct efficiently, such that the secret can be recovered to arbitrary precision, provided the initial squeezing is high enough. The decoding only

* fra.arzani@gmail.com

requires Gaussian resources, considered relatively easy to implement experimentally [34, 35]. We show that in the optical case, decoding can be achieved by interferometry, homodyne detection and a fixed number of single-mode squeezers. We stress that our results follow from simple linear algebra and general considerations on the number of modes.

These results have immediate experimental and technological applications. Indeed, they imply that almost any experimental setup involving squeezed states can be used for QSS. Moreover, small deviations of the setup from a theoretical target one are not important, as long as they can be characterized. This opens the possibility to share resource states securely over a network of CV systems with arbitrarily distributed entanglement links, which may pave the way to server-client architectures for CV-quantum computation. But the relevance of CV random codes is not limited to their practicality. Optimality of random erasure correcting codes for qubits was used in a seminal article to estimate the rate of information leakage from black holes through Hawking radiation [12]. The most relevant objects in this setting are however fields, namely CV systems. This stimulated work applying CV techniques, notably related to QSS, in relativistic contexts [13–16]. The existence of efficient CV random QSS codes may open new avenues for tackling the black-hole information puzzle and related fundamental questions.

The remainder of the article is structured as follows. Some background information is recalled in Sec. II. In Sec. III we describe the encoding procedure the dealer uses to share the secret with all players. In Sec. IV we derive conditions ensuring that any sufficiently large group of players can retrieve the secret state. The decoding operations that the players can carry out when these conditions are satisfied are further described in Sec. V. A precise formulation of our main result is given in Sec. VI together with a sketch of the proof. In an ideal setting, access parties should get full information about the secret and adversaries should get none. As it is often the case in CV, the ideal situation is never achieved in physical scenarios where only finite squeezing is available. Sec. VII and Sec. VIII discuss the amount of information retrieved by the authorized players and the adversaries, respectively, in the finite squeezing scenario. Final remarks in Sec. IX conclude the article. More details about the derivations can be found in the Appendices.

II. CV QUANTUM OPTICS

A convenient way to study an n mode bosonic system is through the $2n$-dimensional phase space. The $2n$ components of the quadrature vector $\boldsymbol{\xi} = \left(\boldsymbol{q}^T, \boldsymbol{p}^T\right)^T$ are the position and momentum operators, obeying the canonical commutation relations

$$[\xi_j, \xi_l] = iJ^{(n)}_{jl}, \tag{1}$$

with $J^{(n)}$ the standard symplectic form

$$J^{(n)} = \begin{pmatrix} \mathbf{0}_n & \mathbb{I}_n \\ -\mathbb{I}_n & \mathbf{0}_n \end{pmatrix}, \tag{2}$$

$\mathbf{0}_n$ and $\mathbb{I}_n$ being zero and identity $n\times n$ matrices. The state of a n-mode system is characterized by its Wigner function $W(\boldsymbol{q}, \boldsymbol{p})$ [1], a quasi-probability distribution defined on phase-space [34]. Gaussian states are naturally defined as those the Wigner function of which is Gaussian, and they are fully characterized by the mean and covariance matrix of the quadrature vector $\boldsymbol{\xi}$.

Gaussian transformations—preserving the Gaussian character of the state—are an essential subset of physical transformations, since they can be implemented deterministically in quantum optics experiments with existing technologies. Unitary Gaussian transformations are elegantly described by the formalism of symplectic matrices. In the Heisenberg picture, the action of a unitary Gaussian operation U_G can be expressed with a slight abuse of notation as a linear map[23, 34]

$$U_G^\dagger \boldsymbol{\xi} U_G = S\boldsymbol{\xi} + \boldsymbol{\eta}, \tag{3}$$

where S is a $2n \times 2n$ real symplectic matrix and $\boldsymbol{\eta}$ is a vector of real numbers [36]. Symplectic matrices acting on n modes are the matrices S preserving the standard symplectic form: $SJ^{(n)}S^T = J^{(n)}$. Under matrix multiplication, they form the group $\mathrm{Sp}(2n, \mathbb{R})$. If displacements are included, amounting to phase-space translations, one gets the so-called inhomogeneous symplectic group. Of specific interest are squeezing and passive operations. Squeezing does not conserve photon number [34] and is usually realized through nonlinear optical processes. Independent squeezing operations on each mode are represented by diagonal symplectic matrices $K = \mathrm{diag}\left(e^{r_1}, \ldots, e^{r_n}, e^{-r_1}, \ldots, e^{-r_n}\right)$, where r_i is the squeezing parameter of mode i [37]. Passive operations are defined as photon-number preserving Gaussian unitaries and correspond to linear optics, represented by the subgroup $L(n) = \mathrm{Sp}(2n, \mathbb{R}) \cap \mathrm{O}(2n)$ of orthogonal, symplectic matrices [36]. Each $S_L \in L(n)$ corresponds to a $n \times n$ unitary matrix $X + iY \in U(n)$ such that

$$S_L = \begin{pmatrix} X & -Y \\ Y & X \end{pmatrix}. \tag{4}$$

This allows us to speak interchangeably of passive interferometers or the corresponding symplectic and unitary matrices.

We recall for later convenience that given two vectors $\boldsymbol{x},\ \boldsymbol{y} \in \mathbb{R}^{2n}$, their symplectic product is defined as

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle \equiv \boldsymbol{x}^T J^{(n)} \boldsymbol{y}. \tag{5}$$

[1] Here, $\mathbf{q}$ and $\mathbf{p}$ are *real*-valued n dimensional vectors, not vectors of operators. In the following we use the same symbols for vectors of quadrature operators and phase-space variables, the meaning should be clear from the context.

We denote by $\boldsymbol{x}\cdot\boldsymbol{y}$ the ordinary Euclidean product $\boldsymbol{x}\cdot\boldsymbol{y} = \sum_j x_j y_j$ and by $\|\boldsymbol{x}\| = \sqrt{\boldsymbol{x}\cdot\boldsymbol{x}}$ the Euclidean norm. Note that, formally, taking the dot product between a vector of real numbers and the vector of quadratures results in a linear combination of quadrature operators. The commutator between two such combinations is simply related to the symplectic product of the vectors

$$[\boldsymbol{x}\cdot\boldsymbol{\xi}, \boldsymbol{y}\cdot\boldsymbol{\xi}] = i\langle \boldsymbol{x}, \boldsymbol{y}\rangle \tag{6}$$

as can be checked using Eq. (1). A basis $\{\boldsymbol{x}_j\}$ of $\mathbb{R}^{2n}$ such that $\langle \boldsymbol{x}_j, \boldsymbol{x}_l\rangle = J^{(n)}_{jl}$ is called *symplectic basis*.

III. ENCODING

We consider the following encoding scheme (see Fig. 1): the dealer couples m modes in a secret state ρ_{s} to n squeezed modes in a passive interferometer described by the symplectic matrix S_L. We assume that each mode's momentum quadrature is squeezed ($r_i > 0$). This simplifies the notation but implies no loss of generality, as local phase-space rotations aligning the squeezing directions correspond to linear optics and can be included in the interferometer.

We denote the vector containing all input quadratures by $\boldsymbol{\xi}^{\mathrm{in}} = \left((\boldsymbol{q}^{\mathrm{sqz}})^T, (\boldsymbol{q}^{\mathrm{s}})^T, (\boldsymbol{p}^{\mathrm{sqz}})^T, (\boldsymbol{p}^{\mathrm{s}})^T\right)^T$ where the quadratures of the jth squeezed mode are related to the vacuum quadratures by $q_j^{\mathrm{sqz}} = e^{r_j} q_j^{(0)}$, $p_j^{\mathrm{sqz}} = e^{-r_j} p_j^{(0)}$. After the interferometer the vector of quadrature operators is transformed as

$$\boldsymbol{\xi}^{\mathrm{net}} = \begin{pmatrix} \boldsymbol{q}^{\mathrm{net}} \\ \boldsymbol{q}^{\mathrm{d}} \\ \boldsymbol{p}^{\mathrm{net}} \\ \boldsymbol{p}^{\mathrm{d}} \end{pmatrix} = S_L \boldsymbol{\xi}^{\mathrm{in}} = \begin{pmatrix} X & -Y \\ Y & X \end{pmatrix} \boldsymbol{\xi}^{\mathrm{in}}. \tag{7}$$

One of the output modes of the interferometer is then sent to each of the players.

IV. DECODABILITY CONDITIONS

We now investigate the conditions that the symplectic matrix S_L must satisfy and the relations between k, m and n in order for any set of k or more players to be able to access the secret quadratures. Specifically, for each authorized set we look for $2m$ independent linear combinations of quadratures that do not involve the antisqueezed quadratures q_j^{sqz} and contain one of the secret quadratures each. We will later show that if such combinations exist, all information about the secret can be accessed by any group of k or more players. We will require $k \geq m$, otherwise the players cannot reconstruct a general state of m modes.

Consider a subset of players $A = \{a_1,\ a_2,\ \ldots,\ a_k\}$ who are given the modes with quadratures

$$\boldsymbol{\xi}^A = \begin{pmatrix} \boldsymbol{Q}^A \\ \boldsymbol{P}^A \end{pmatrix}, \quad \begin{aligned} \boldsymbol{Q}^A &= \left(q^{\mathrm{net}}_{a_1},\ q^{\mathrm{net}}_{a_2},\ \ldots,\ q^{\mathrm{net}}_{a_k}\right)^T, \\ \boldsymbol{P}^A &= \left(p^{\mathrm{net}}_{a_1},\ p^{\mathrm{net}}_{a_2},\ \ldots,\ p^{\mathrm{net}}_{a_k}\right)^T. \end{aligned} \tag{8}$$

A need to cancel the contribution of the antisqueezed quadratures. Let us rewrite Eq. (7) as

$$\boldsymbol{\xi}^A = M^A \boldsymbol{q}^{\mathrm{sqz}} + N^A \boldsymbol{p}^{\mathrm{sqz}} + H^A \boldsymbol{\xi}^{\mathrm{s}} \tag{9}$$

where the entries of the matrices M^A, N^A, and H^A are defined by the coefficients of S_L and $\boldsymbol{\xi}^{\mathrm{s}}$ collects the secret quadratures. Any linear combination of the $\boldsymbol{\xi}^A$s can be written $\boldsymbol{v}^T\boldsymbol{\xi}^A$ with $\boldsymbol{v} \in \mathbb{R}^{2k}$. According to Eq. (9), the product $\boldsymbol{v}^T\boldsymbol{\xi}^A$ does not contain any antisqueezed quadrature iff $\boldsymbol{v}$ lies in the kernel of $\left(M^A\right)^T$. By construction, M^A has $2k$ rows and n columns, therefore

$$\dim\left(\ker(M^A)^T\right) \geq 2k - n \tag{10}$$

Then, if $k \geq m + \lceil \frac{n}{2} \rceil$ it is always possible to find $2m$ linearly independent vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{2m} \in \ker\left(M^A\right)^T$ (here $\lceil x \rceil$ denotes the smallest integer greater than or equal to x). Let us suppose this condition is satisfied and organise the vectors $\boldsymbol{v}_j$ as rows of a matrix R. Applying R to $\boldsymbol{\xi}^A$ we get

$$\begin{aligned} R\boldsymbol{\xi}^A &= RM^A\boldsymbol{q}^{\mathrm{sqz}} + RN^A\boldsymbol{p}^{\mathrm{sqz}} + RH^A\boldsymbol{\xi}^{\mathrm{s}} && (11) \\ &\equiv RN^A\boldsymbol{p}^{\mathrm{sqz}} + T\boldsymbol{\xi}^{\mathrm{s}} && (12) \end{aligned}$$

where the last line defines the $2m \times 2m$ matrix $T = RH^A$. The access party A can then decode the secret iff T is invertible. Indeed, multiplying T^{-1} by Eq. (12) and defining $D \equiv T^{-1}R$, $B = T^{-1}RN^A$, leads to

$$D\boldsymbol{\xi}^A = B\boldsymbol{p}^{\mathrm{sqz}} + \boldsymbol{\xi}^{\mathrm{s}}. \tag{13}$$

So when A measure the linear combination of quadratures defined by the jth row of D, the outcomes will follow the same probability distribution as ξ^{s}_j, apart from random displacements drawn from a Gaussian probability distribution, due to the term $B\boldsymbol{p}^{\mathrm{sqz}}$. These displacements decrease with increasing input squeezing, ultimately vanishing for infinite squeezing. In this limit, the access party can perfectly sample from the original secret state. Note that real linear combinations of the rows of D are linear combinations of the ξ^{s}_j plus the squeezed quadratures, so A can also measure arbitrary quadratures of the secret (see below). An alternative description based on Wigner functions can be found in Appendix C 1.

In summary, A can reconstruct the secret if it is composed of at least $m + \lceil \frac{n}{2} \rceil$ players and the matrix T in Eq. (12) is not singular.

Given any linear optical network S_L, these two conditions determine the authorized subsets of players, that is the access structure. It is not necessary to construct T explicitly to check whether $\det T \neq 0$ as we show in Appendix A that this is equivalent to $\det\left(M^A\ H^A\right) \neq 0$. The latter condition explicitly involves the coefficients of S_L, which will be useful to prove our main result.

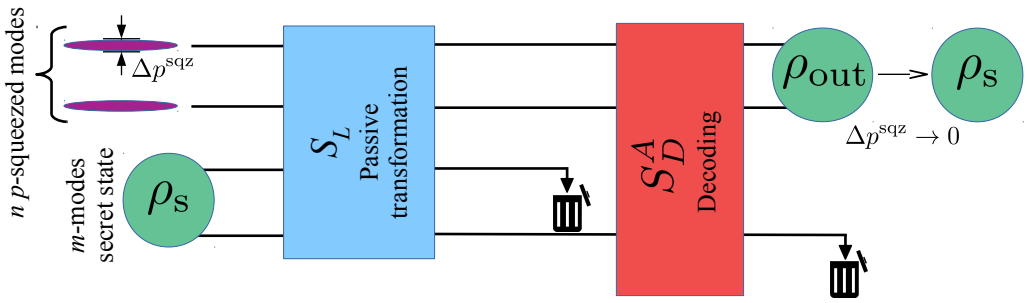


FIG. 1. A sketch of the encoding procedure with $n = 2$, $m = 2$, followed by decoding from the share of the access party consisting of the first, second and fourth mode, while the third mode, corresponding to an adversary, is discarded. As shown in the Sec. IV, the secret can be recovered from any $m + \lceil \frac{n}{2} \rceil = 3$ out of the four modes. The decoded state ρ_{out} converges to the secret state ρ_{s} as the input squeezing increases and the last mode can also be discarded after the decoding (see Sec. V).

V. DECODING

We now clarify in which sense the above conditions allow the access party to decode the secret. Consider an access party A and suppose the conditions in the previous section are met. Clearly, A can measure the linear combinations defined by $D\boldsymbol{\xi}^A$ by combining the results of local homodyne detections. Indeed, Eq. (13) can be rewritten

$$\xi_j^{\mathrm{s}} + \sum_{l=1}^{n} B_{jl} p_l^{\mathrm{sqz}} = \sum_{l=1}^{k} \left(D_{jl} Q_l^A + D_{j,l+k} P_l^A \right) \tag{14}$$

$$= \sum_{l=1}^{k} \alpha_{jl} \left(\cos\theta_{jl} Q_l^A + \sin\theta_{jl} P_l^A \right) \tag{15}$$

for appropriately chosen $\alpha_{jl}, \theta_{jl} \in \mathbb{R}$. A achieve their goal by measuring the rotated quadratures with angles θ_{jl} and summing their results multiplied by α_{jl}. Since the same reasoning applies to any linear combination of the ξ_js, A can perform an arbitrary homodyne measurement of the secret ρ_{s}. Sampling any quadrature from ρ_{s} allows A to simulate any protocol needing homodyne measurements of ρ_{s}, from quantum key distribution [38], to measurement based quantum computing [39], to, when provided with several copies of ρ_{s}, tomography or verification [40].

Moreover, A can physically reconstruct the secret state by applying a Gaussian unitary transformation. Let us call $\boldsymbol{\xi}^{\mathrm{out}} \equiv D\boldsymbol{\xi}^A$. Since the secret quadratures are conjugated canonical operators we have

$$\left[\xi_j^{\mathrm{out}}, \xi_l^{\mathrm{out}}\right] = \left[\xi_j^{\mathrm{s}}, \xi_l^{\mathrm{s}}\right] = i J_{jl}^{(m)}. \tag{16}$$

Since S_L is symplectic, we also have $\left[\xi_j^A, \xi_l^A\right] = i J_{jl}^{(k)}$. Using $\boldsymbol{\xi}^{\mathrm{out}} = D\boldsymbol{\xi}^A$ leads to

$$\left[\xi_j^{\mathrm{out}}, \xi_l^{\mathrm{out}}\right] = i \left(D J^{(k)} D^T \right)_{jl} = i J_{jl}^{(m)}. \tag{17}$$

so the rows of D are vectors from a symplectic basis of $\mathbb{R}^{2k}$ [41] the span of which has dimension $2m$. They can be completed to a symplectic basis of $\mathbb{R}^{2k}$ through a Gram-Schmidt-like procedure where the scalar product is replaced by the symplectic product [41]. Alternatively, the procedure explained in Appendix B can be used, improving on the number of required single-mode squeezers (see below). Let us call S_D^A the symplectic matrix the first m and $(k+1)$st to $(k+m)$th rows of which are the rows of D, while the others are constructed by one of the above mentioned procedures. Its action on the vector of $2k$ quadratures of the access party A corresponds to a unitary Gaussian transformation U_D^A such that

$$\left(U_D^A\right)^\dagger \boldsymbol{\xi}^A U_D^A = S_D^A \boldsymbol{\xi}^A. \tag{18}$$

By construction, the first m position and momentum entries of $S_D^A \boldsymbol{\xi}^A$ correspond to $\boldsymbol{\xi}^{\mathrm{out}}$, so if A apply the physical evolution corresponding to U_D^A and S_D^A, they end up with m modes in the secret state, apart from finite squeezing contributions.

Note that S_D^A may, and generally does, involve squeezing. However, remarkably, the procedure detailed in Appendix B always allows one to construct S_D^A involving a passive interferometer acting on the k modes of A, $2m$ independent single-mode squeezers and a final passive interferometer. For $m = 1$ (single-mode secrets), the number of squeezers can be further reduced to one per access party by replacing the second one with a homodyne measurement followed by an optical displacement depending on the measurement result. Note that the number of squeezers per access party in the decoding does not scale with the number of players. This result generalizes the result of [25] to all passive interferometers, including the ones mixing positions and momenta, and to secrets of any size. The generalization beyond orthogonal transformations of the position operators is essential for the result stated in the next section.

VI. ALMOST ANY INTERFEROMETER CAN BE USED FOR QSS

We can now formalize our main result: the encoding and decoding schemes outlined in the previous sections define a secret sharing scheme for almost all passive interferometers S_L, in the sense of the Haar measure, that is the constant measure on $L(n)$. In other words, if S_L is drawn uniformly at random from all possible interferometers on n modes, any group of k or more players will almost surely be able decode a secret state of m-modes, provided $k \geq m + \lceil \frac{n}{2} \rceil$. A sketch of the proof, detailed in Appendix D, follows.

Let $\mathcal{B}$ be the set of matrices that *cannot* be used for secret sharing. For $S_L \in L(n)$ to be in $\mathcal{B}$, $\det\left(M\ H^A\right) = 0$ for at least one access party A, which we denote $S_L \in \mathcal{B}^A$. Because of positivity and countable additivity, we have for the Haar measure of $\mathcal{B}$, $\mu_H(\mathcal{B}) \leq \sum_A \mu_H\left(\mathcal{B}^A\right)$ and we just need to show that each $\mathcal{B}^A$ has zero measure. Each of them is defined as the zero set of a polynomial function of the coefficients of S_L (the determinant of a submatrix), which, regarding $U(n)$ as a manifold, identifies a lower dimensional set, which has zero measure [42]. In other words, since $L(n)$ is a Lie group of dimension n^2, it can be parametrized by n^2 real variables defined in an appropriate region $\mathcal{E} \subset \mathbb{R}^{n^2}$. The entries of S_L can be written as polynomials of trigonometric functions of n^2 angles $\boldsymbol{\lambda}$, so the $\det\left(M\ H^A\right)$ is a real analytic function [43, 44] of $\boldsymbol{\lambda}$, whose zero set has necessarily null measure on $\mathcal{E}$ [44, 45]. Therefore $\mathcal{B}$ has zero Haar measure in $L(n)$. Up to a normalization factor, the Haar measure can be seen as a uniform probability distribution over the unitary group. It follows that if a unitary matrix $\bar{U}$ is chosen uniformly at random, the probability that $\bar{U} \in \mathcal{B}$ is zero.

Note that the *uniformity* property of the Haar measure is not required for the proof: we rather need it to be equivalent to Lebesgue measure on the domain $\mathcal{E}$ of Euler angles, that is if a set has zero measure in $\mathcal{E}$, then it also has zero Haar measure. Our results thus readily apply to any measure that does not assign positive measure to a set of unitaries (interferometers) of zero Haar measure. Moreover, it is not necessary to be able to achieve all possible interferometers in order to find good ones for QSS. To fix the ideas, let us suppose that some experimental setup has continuous parameters $\boldsymbol{u}$ that can be adjusted to apply one of a set of interferometers $U(\boldsymbol{u})$. If $U(\boldsymbol{u})$ spans a set of non-zero Haar measure when $\boldsymbol{u}$ is varied, then almost all configurations will lead to a good encoding for QSS according to our definition.

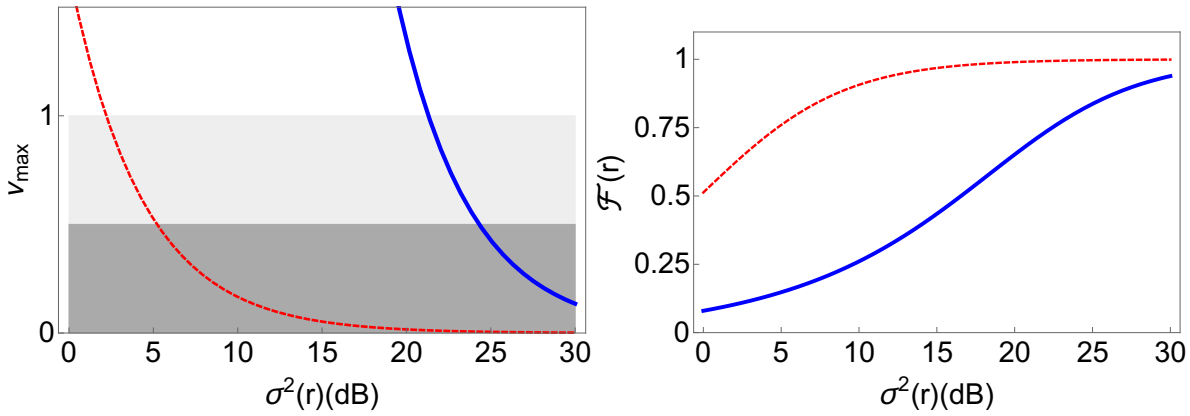
VII. QUALITY OF THE STATE RECONSTRUCTED BY AUTHORIZED SETS

Since both encoding and decoding by any access party require Gaussian resources only, the overall process defines a Gaussian channel [23, 46]. More specifically, as discussed in Appendix C 1, the Wigner function of the output state is the one of the secret state convoluted with a Gaussian filter that depends on the initial squeezing and on the interferometer S_L. Such channels are sometimes referred to as *(additive) classical noise channels* [46]. In the ideal case where infinitely squeezed states are used $\Delta p_j^{\mathrm{sqz}} = 0$, the channel coincides with the identity channel. For finite squeezing, the protocol introduces Gaussian noise that becomes smaller as squeezing is increased. We can characterize the quality of the reconstructed state in the realistic imperfect case by relating the amount of input squeezing to the fidelity between the reconstructed state and the secret. In particular, suppose for simplicity that the secret is a single-mode coherent state, and all the input squeezed states have the same squeezing $\Delta^2 p_j^{\mathrm{sqz}} = e^{-2r}/2 \equiv \sigma^2(r)$. The fidelity of the reconstructed state can then be expressed as (see Appendix C 2)

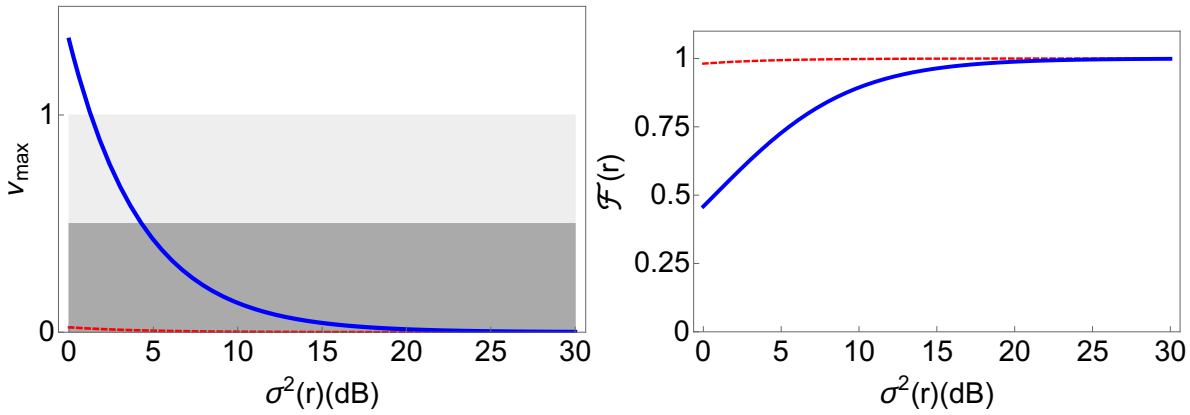
$$\mathcal{F}^A(r) = 1/\sqrt{1 + \sigma^2(r)\,\eta + \sigma^4(r)\,\zeta} \tag{19}$$

where $\eta = \mathrm{Tr}\left(BB^T\right)$, $\zeta = \det\left(BB^T\right)$, and B is defined in Eq. (13). Clearly $\mathcal{F}^A(r) \to 1$ for $r \to \infty$. The same holds for any input state, although the expression of the fidelity is generally not as simple. Another possible way to assess the noise added by the encoding and decoding procedure by one access party is to compute the maximum eigenvalue $\nu_{\max}$ of the noise matrix $\mathcal{N} = B\Delta^2 B^T$, with $\Delta = \mathrm{diag}(\sigma_1, \ldots, \sigma_n)$. This can be interpreted as the size of the smallest features of the secret Wigner function conserved by the channel [47, 48]. Smaller structures (*e.g.* regions of negativity) are blurred out by the convolution. The values 1 and 0.5 can be taken as a references. For $\nu_{\max} > 1$ the channel is known to be entanglement-breaking [48–50], whereas for $\nu_{\max} < 0.5$ a generalization of the no-cloning theorem ensures that the corresponding access party holds the best possible copy of the secret state [51, 52]. Some examples are plotted in Fig. 2. The squeezing required to achieve a good reconstruction quality depends on the interferometer used for the encoding and can in general be very large (in the tens of decibels). This can be seen from Fig. 2a, reporting $\nu_{\max}$ and the fidelity obtained from a randomly chosen interferometer as a function of input squeezing. However, interferometers allowing for good reconstruction with technologically achievable squeezing values [53, 54] do not seem to be rare and can be found by simple random sampling. Figs. 2b, 2c and 2d were for example obtained from the interferometers with the smallest $\nu_{\max}$ from samples of 10^3 interferometers chosen according to the Haar measure. In general it seems that the required squeezing increases with the number of modes involved but a more thorough characterization of the dependence of the required squeezing on the encoding interferometer is left for future work. The matrices representing the interferometers used for the plots are reported in Appendix E.

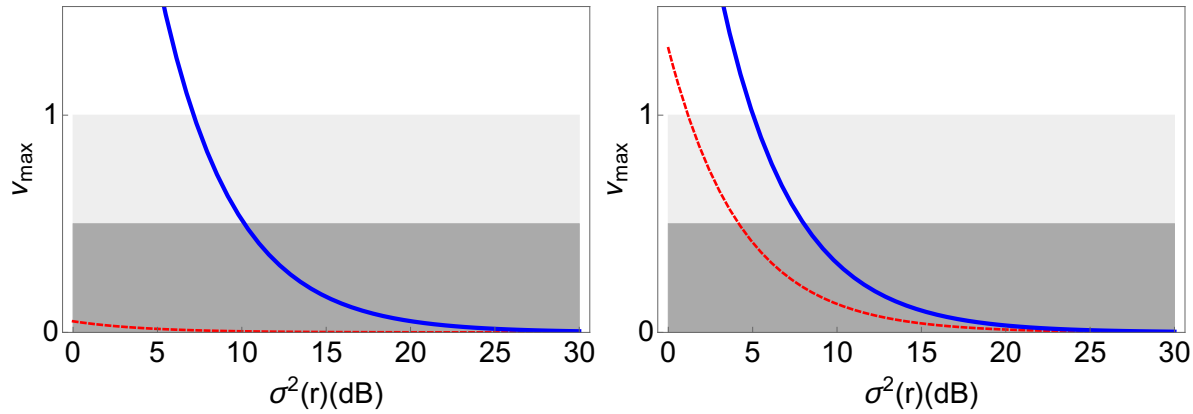
It is worth noting that the quality of the state reconstructed by authorized parties is not affected by the antisqueezing contributions. This means that the same reconstruction quality can be achieved with non pure



(a) $m = 1$, $n = 2$, Haar random



(b) $m = 1$, $n = 2$, best of 10^3 Haar random matrices



(c) $m = 1$, $n = 4$, best of 10^3 Haar random matrices

(d) $m = 2$, $n = 2$, best of 10^3 Haar random matrices

FIG. 2. Quality of the reconstructed state for several interferometers. The blue, solid (red, dashed) lines correspond to the access party whose decoding results in the worst (best) reconstruction of the secret. In the plots of $\nu_{\max}$, the upper, white region $\nu_{\max} > 1$ corresponds to the encoding-decoding channel being entanglement-breaking, while the dark gray region $\nu < 0.5$ corresponds to the access party having the best possible copy of the secret allowed by optimal cloning. The plots (a) and (b) were obtained for two different interferometers and assuming two out of three players are trying to reconstruct a single-mode secret. The plot in (c) is for three out of five players and a single-mode secret, while (d) is for three out of four players trying to reconstruct a two-modes state (the scheme in Fig. 1). The matrices representing the corresponding interferometers are reported in Appendix E.

squeezed states as long as the noise in one quadrature is sufficiently reduced. This particular type of imperfect squeezed states is common in experimental situations. Optical parametric oscillators provide a notable example where the excess noise in the antisqueezed quadrature is larger than the inverse of the noise in the squeezed quadrature (See for example [55]).

If the scheme is used as an ECC, the results of the present section assess how much squeezing is needed to make the secret state robust to the loss of $n+m-k$ modes. For QSS, additional conditions on the unauthorized parties have to be satisfied. This is discussed in the next section.

VIII. UNAUTHORIZED SETS

In QSS, unauthorized parties should get no information about the secret. This is not strictly true in any realistic realization of our scheme, as for any finite value of squeezing, all subsets can get some information about the secret. This is inherent to any CV protocol, as was recently discussed in detail in [56] for a family of single-mode CV-QSS schemes corresponding to a special case of our scheme. As it turns out, in the multi-mode case the access structure is further complicated by the fact that some subsets of less than $m+\lceil\frac{n}{2}\rceil$ players can access some of the secret quadratures even in the infinite-squeezing limit, while groups smaller than a threshold value k^* are prevented from accessing the secret. To see this, let us fix n and m and choose $k=m+\lceil\frac{n}{2}\rceil$. Consider then a set Z of $k-l$ players, with $0<l<k$. Z can construct a matrix M^Z analogous to M^A but of smaller size. Eq.(10) then implies that, for $l<m$, Z can almost always retrieve $2m-2l$ combinations of the secret quadratures free from the antisqueezed contributions. On the other hand, a similar reasoning as that in the Sec. VI shows that this is almost never the case for $l\geq m$: groups of $k-m$ players or less cannot obtain any linear combinations free of all antisqueezing contributions. This implies that they get no information about the secret for infinite input squeezing, as the antisqueezing contributions add white noise to their quadratures. For $m=1$ our scheme defines then a (k,n) threshold scheme [19], where the adversary structure is composed of all complements of an authorized set. In the general case, the size of the sets that obtain no information about the secret (for infinite squeezing) depends on the size of the latter: any set of k or more players can reconstruct the full secret and sets of $k^*=k-m$ or less players are denied all information about it. Such schemes are known in the DV literature as ramp schemes [57] (note that the same term is used with a different meaning in [56], where only single-mode secrets are considered and the focus is on the information leakage due to finite squeezing). The amount of information leaked to the adversaries is also constrained by the fidelity of the state reconstructed by the access party with the secret, since the fidelity of the states reconstructed by disjoint sets of players is limited by optimal cloning. Notably, as mentioned above, increasing the noise of antisqueezed quadratures at fixed squeezing, the reconstruction by the authorized parties is unaffected, while that of the unauthorized party degrades.

IX. CONCLUSIONS

We have introduced a random coding scheme for sharing multimode bosonic states using Gaussian resources. The possibility of using almost any interferometer gives plenty of room for optimization and implies that potentially any experimental setup producing multi-mode squeezed states can be used for QSS, paving the way to quantum resource sharing across entangled networks with arbitrary topology. In particular, this may have applications for sharing resource states in server-client architectures for optical quantum computing [58, 59], which is an increasingly studied paradigm, due to the difficulty of producing genuinely quantum resources for quantum supremacy [60, 61]. From the perspective of error correction [21, 62],we can affirm that a Haar randomly chosen linear interferometer acts as an optimal erasure code, since any code tolerating the loss of a higher number of modes would violate no-cloning.

ACKNOWLEDGMENTS

F. A. is grateful to Luca A. Ardigò and Nicolas Treps for fruitful discussions and to Lorenzo Posani for valuable feedback on earlier versions of the manuscript. We acknowledge financial support from the BPI France project 143024 RISQ and the French National Research Agency project ANR-17-CE24-0035 VanQuTe.

Appendix A: Equivalent condition for invertibility of the matrix T

The decodability conditions derived in the main text are readily computed once S_L is known but checking whether the matrix T (defined in Eq. (12) of the main text) is invertible requires the explicit calculation of a basis of the kernel of $\left(M^A\right)^T$ (see Eq. (9)), which is not very practical. We prove here a condition equivalent to the invertibility of T in the case that M^A has full rank: $\mathrm{rank}\left(M^A\right)=n-m$. The condition results in a polynomial equation in the coefficients of M^A and thus does not require computing the kernel of $\left(M^A\right)^T$ explicitly. This will be particularly useful for the proof of our main result.

Let us call $V=\mathrm{Ker}\left(\left(M^A\right)^T\right)\subset\mathbb{R}^{2k}$. If M^A has full rank, then $\dim(V)=2k-n+m=2m$, since M^A always has $2k$ rows and $n-m$ columns (we assume $k=m+\lceil\frac{n}{2}\rceil$). Let us denote by $\boldsymbol{h}_j=H^A(j)$ the jth column of H^A and by $\boldsymbol{h}_j\big|_V$ its projection on V (see Eq. (9) for the definition of H^A). Let us introduce a basis of V, $\{v_1,\ldots,v_{2m}\}$. We

can assume without loss of generality that these vectors are the rows of the matrix R in the main text. Then

$$\boldsymbol{h}_j = \boldsymbol{h}_j\big|_V + \boldsymbol{h}_j\big|_{V^\perp} = \sum_l (\boldsymbol{v}_l \cdot \boldsymbol{h}_j)\, \boldsymbol{v}_l + \boldsymbol{a}_j = \sum_l T_{lj} \boldsymbol{v}_l + \boldsymbol{a}_j \tag{A1}$$

by definition of T, with $\boldsymbol{a}_j = \boldsymbol{h}_j\big|_{V^\perp}$. Consider now the square matrix

$$\left(M^A \middle| H^A\right) = \left(M^A \middle| \boldsymbol{h}_1 \middle| \ldots \middle| \boldsymbol{h}_{2m}\right) \tag{A2}$$

where the notation specifies the last $2m$ columns. Since the determinant is a multilinear, alternating function of the columns we have

$$\begin{aligned}
\det\left(M^A\ H^A\right) &= \det\left(M^A \middle| \boldsymbol{h}_1 \middle| \ldots \middle| \boldsymbol{h}_{2m}\right) = \det\left(M^A \middle| \sum_{l_1} T_{l_1,1}\boldsymbol{v}_{l_1} \middle| \ldots \middle| \sum_{l_{2m}} T_{l_{2m},2m}\boldsymbol{v}_{l_{2m}}\right) \\
&= \sum_{l_1,\ldots,l_{2m}} T_{l_1,1}\ldots T_{l_{2m},2m} \det\left(M^A \middle| \boldsymbol{v}_{l_1} \middle| \ldots \middle| \boldsymbol{v}_{l_{2m}}\right) = \sum_{l_1,\ldots,l_{2m}} T_{l_1,1}\ldots T_{l_{2m},2m}\epsilon_{l_1,\ldots,l_{2m}} \det\left(M^A\ |\boldsymbol{v}_1 \mid \ \ldots\ \mid \boldsymbol{v}_{2m}\right) \\
&= \det(T)\det\left(M^A \middle| \boldsymbol{v}_1 \middle| \ldots \middle| \boldsymbol{v}_{2m}\right)
\end{aligned} \tag{A3}$$

where $\epsilon_{l_1,\ldots,l_{2m}}$ is the completely antisymmetric tensor. The second line follows from the fact that, since M^A is full rank, $V^\perp = \mathrm{span}\left(\left\{M^A(j)\right\}\right)$ (in other words, V is the space of the vectors orthogonal to all the rows of $\left(M^A\right)^T$). This means that in particular each $\boldsymbol{a}_j$ is a linear combination of the rows of M^A so terms containing any of the $\boldsymbol{a}_j$ give zero contribution to the determinant. Since by hypothesis $\det\left(M^A\ |\boldsymbol{v}_1 \mid \ \ldots\ \mid \boldsymbol{v}_{2m}\right) \neq 0$, it follows that

$$\det(T) \neq 0 \iff \det\left(M^A\ H^A\right) \neq 0. \tag{A4}$$

Since M^A and H^A are defined in terms of the coefficients of S_L and the determinant is a polynomial function thereof, this is the condition we were looking for.

Appendix B: Extending the matrix D to a symplectic matrix

We outline here an algorithm that can be used to extend the matrix D in Eq. (13) for an access party A to a symplectic operation S_D^A corresponding to a physical, unitary Gaussian operation that the access party can implement to output a subsystem in the secret state (apart from terms vanishing for high enough squeezing). It is instructive to begin detailing the case of a single-mode secret state, $m = 1$. The general case is treated in subsection B 2.

Given a subspace $\mathcal{V} \subseteq \mathbb{R}^{2n}$, we will call *symplectic complement* the linear space

$$\mathcal{V}^J \equiv \left\{w \in \mathbb{R}^{2n} : \langle \boldsymbol{v}, \boldsymbol{w}\rangle = 0\ \forall\ v \in \mathcal{V}\right\}. \tag{B1}$$

We will reserve the notation $\mathcal{V}^\perp$ and the phrase *orthogonal complement* to indicate the orthogonal complement with respect to the Euclidean product

$$\mathcal{V}^\perp \equiv \left\{w \in \mathbb{R}^{2n} : \boldsymbol{v} \cdot \boldsymbol{w} = 0\ \forall\ v \in \mathcal{V}\right\}. \tag{B2}$$

1. Single mode secret state

Let us start from the rows of the matrix D defined in Eq. (13). For $m = 1$, D only has two rows, which we denote by $\boldsymbol{x}$ and $\boldsymbol{y}$. By construction we have

$$\begin{aligned}
\boldsymbol{x} \cdot \boldsymbol{\xi}^A &= q^{\mathrm{out}} = q^{\mathrm{s}} + \sum_j B_{1j} p_j^{\mathrm{sqz}} \\
\boldsymbol{y} \cdot \boldsymbol{\xi}^A &= p^{\mathrm{out}} = p^{\mathrm{s}} + \sum_j B_{2j} p_j^{\mathrm{sqz}}
\end{aligned} \tag{B3}$$

where the matrix B is also defined in Eq. (13). Our goal is to find $2k-2$ vectors to add as rows of the matrix D such that the resulting matrix is symplectic. To do so, first define

$$\boldsymbol{x}_1 = \frac{\boldsymbol{x}}{\|\boldsymbol{x}\|} \tag{B4}$$

and $\boldsymbol{y}_1 = -J^{(k)}\boldsymbol{x}_1$. The vectors $\boldsymbol{x}_1$ and $\boldsymbol{y}_1$ are both normalized and their symplectic product is $\langle \boldsymbol{x}_1, \boldsymbol{y}_1\rangle = 1$, since $\left(J^{(k)}\right)^2 = -\mathbb{I}_{2k}$. Using Eq. (6) we see that the operators $q_1 = \boldsymbol{x}_1 \cdot \boldsymbol{\xi}^A$ and $p_1 = \boldsymbol{y}_1 \cdot \boldsymbol{\xi}^A$ have the correct canonical commutator $[q_1, p_1] = i$.

Consider now $\mathcal{V}_1 \equiv \mathrm{span}\left\{\boldsymbol{x}_1, \boldsymbol{y}_1\right\} \subseteq \mathbb{R}^{2k}$ and a normalized vector $\boldsymbol{x}_2 \in \mathcal{V}_1^\perp$, that is

$$\boldsymbol{x}_2 \cdot \boldsymbol{x}_1 = \boldsymbol{x}_2 \cdot \boldsymbol{y}_1 = 0; \quad \|\boldsymbol{x}_2\| = 1. \tag{B5}$$

Since $\left(J^{(k)}\right)^2 = -\mathbb{I}_{2k}$, these conditions imply that $\boldsymbol{x}_2$ has null symplectic product with both $\boldsymbol{x}_1$ and $\boldsymbol{y}_1$. Moreover, the vector $\boldsymbol{y}_2 \equiv -J^{(k)}\boldsymbol{x}_2$ is also normalized, orthogonal to $\boldsymbol{x}_1$, $\boldsymbol{x}_2$ and $\boldsymbol{y}_1$, has null symplectic product with $\boldsymbol{x}_1$ and $\boldsymbol{y}_1$ and satisfies $\langle \boldsymbol{x}_2, \boldsymbol{y}_2\rangle = 1$. This is a consequence of $\mathcal{V}_1^\perp = \mathcal{V}_1^J$ and the fact that each multiplication by J transforms Euclidean scalar products into symplectic ones and vice versa, up to a sign. The argument can be repeated for $\mathcal{V}_2 \equiv \mathrm{span}\left\{\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{y}_1, \boldsymbol{y}_2\right\} \subseteq \mathbb{R}^{2k}$ and a normalized $\boldsymbol{x}_3 \in \mathcal{V}_2^\perp$ and so on, until $\mathcal{V}_k^\perp = \{\boldsymbol{0}\}$. The

matrix $O_1 = (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k, \boldsymbol{y}_1, \ldots, \boldsymbol{y_k})^T$ is orthogonal and symplectic by construction, and corresponds to a linear optics transformation leaving the position of the first mode in the secret position, up to a rescaling. The correct scaling can be obtained applying a single-mode squeezer to the first mode, with symplectic matrix $K_1 = \|\boldsymbol{x}\| \oplus \mathbb{I}_{k-1} \oplus \frac{1}{\|\boldsymbol{x}\|} \oplus \mathbb{I}_{k-1}$.

We now have to ensure that the first mode's momentum is mapped to the secret momentum. Since the rows of $K_1 O_1$ are a basis of $\mathbb{R}^{2k}$, we can write

$$\boldsymbol{y} = \alpha_1 \boldsymbol{x} + \sum_{j=2}^{k} \alpha_j \boldsymbol{x}_j + \frac{\beta_1}{\|x\|} \boldsymbol{y}_1 + \sum_{j=2}^{k} \beta_j \boldsymbol{y}_j. \tag{B6}$$

It is easy to check that $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = 1$ implies $\beta_1 = 1$, so

$$\boldsymbol{y}_1' \equiv \frac{\boldsymbol{y}_1}{\|\boldsymbol{x}\|} = \boldsymbol{y} - \alpha_1 \boldsymbol{x} - \sum_{j=2}^{k} \alpha_j \boldsymbol{x}_j - \sum_{j=2}^{k} \beta_j \boldsymbol{y}_j. \tag{B7}$$

Our goal is achieved if we find a symplectic transformation that maps $\boldsymbol{y}_1' \mapsto \boldsymbol{y}$ leaving $\boldsymbol{x}$ unchanged. This is realized in three steps. First, a shear [39] can be applied on the first mode to remove the $\boldsymbol{x}$ term. The transformation corresponds to the Gaussian unitary $\exp\left(i\alpha_1 \boldsymbol{q}_1'^2\right)$, where $\boldsymbol{q}_1'$ is the position operator of the first mode after $K_1 O_1$ has been applied. The corresponding symplectic matrix is

$$K_S = \begin{pmatrix} & \mathbb{I}_k & & 0_k \\ \alpha_1 & 0 & \ldots & 0 & \\ 0 & 0 & \ldots & 0 & \\ & \vdots & & & \mathbb{I}_k \\ 0 & 0 & \ldots & 0 & \end{pmatrix}. \tag{B8}$$

Next, rewrite

$$\sum_{j=2}^{k} \alpha_j \boldsymbol{x}_j + \sum_{j=2}^{k} \beta_j \boldsymbol{y}_j = \sum_{j=2}^{k} \eta_j \left(\cos\theta_j \boldsymbol{x}_j - \sin\theta_j \boldsymbol{y}_j\right) \tag{B9}$$

and apply mode-wise rotations (phase-shifts) that map

$$\begin{aligned} \boldsymbol{x_j} &\mapsto \boldsymbol{x}_j' = \cos\theta_j \boldsymbol{x}_j - \sin\theta_j \boldsymbol{y}_j \\ \boldsymbol{y_j} &\mapsto \boldsymbol{y}_j' = \sin\theta_j \boldsymbol{x}_j + \cos\theta_j \boldsymbol{y}_j, \end{aligned} \tag{B10}$$

which is a passive transformation corresponding to the symplectic matrix

$$O_2 = \begin{pmatrix} 1 & 0 & \ldots & 0 & 0 & \ldots \\ 0 & & & 0 & & \\ \vdots & & X_2 & \vdots & & -Y_2 \\ 0 & 0 & \ldots & 1 & 0 & \ldots \\ 0 & & & 0 & & \\ \vdots & & Y_2 & \vdots & & X_2 \end{pmatrix}. \tag{B11}$$

with $X_2 = \operatorname{diag}(\cos\theta_2, \ldots, \cos\theta_k)$, $Y_2 = \operatorname{diag}(\sin\theta_2, \ldots, \sin\theta_k)$. Finally, apply $k-1$ controlled-Z operations [39] between the first and each of the other modes, of the form $\exp\left(i\eta_j q_1' \otimes q_j'\right)$ with $q_j' = \boldsymbol{x}_j' \cdot \boldsymbol{\xi}^A$, $q_1' = \boldsymbol{x} \cdot \boldsymbol{\xi}^A = q^{\text{out}}$. Each of these two-modes operations acts as

$$e^{-i\eta_j q_1' \otimes q_j'} \begin{pmatrix} q_1' \\ q_j' \\ p' \\ p_j' \end{pmatrix} e^{i\eta_j q_1' \otimes q_j'} = \begin{pmatrix} q_1' \\ q_j' \\ p' + \eta_j q_j' \\ p_j' + \eta_j q_1' \end{pmatrix} \tag{B12}$$

where $p' = \boldsymbol{y}' \cdot \boldsymbol{\xi}^A$. Since $\left[q_j', q_l'\right] = 0$ the C_Z operations can be performed in any order, and the resulting symplectic matrix is

$$K_2 = \begin{pmatrix} & \mathbb{I}_k & & 0_k \\ 0 & \eta_2 & \eta_3 & \ldots & \\ \eta_2 & 0 & 0 & \ldots & \mathbb{I}_k \\ \vdots & & \ddots & & \end{pmatrix}. \tag{B13}$$

Reconstruction of the secret state at mode one is then achieved by the sequence of transformations corresponding to

$$S_D^A = K_2 O_2 K_S K_1 O_1. \tag{B14}$$

This procedure is not efficient in terms of squeezers, as each controlled-Z requires squeezing, and the overall number of independent squeezers required for the above procedure is only upper bounded by the number of modes: it never exceeds k, since we could apply the Bloch-Messiah reduction (also known as Euler decomposition) [36, 63] to S_D^A.

We can however reduce the number of squeezers by the following strategy. Instead of K_2, after O_2 one could apply a passive transformation that maps

$$\boldsymbol{x}_2' \mapsto \boldsymbol{x}_2'' \propto \sum_{j=2}^{k} \eta_j \left(\cos\theta_j \boldsymbol{x}_j - \sin\theta_j \boldsymbol{y}_j\right) = \sum_{j=2}^{k} \eta_j \boldsymbol{x}_j'. \tag{B15}$$

This is always possible, as it amounts to finding a basis of $\mathbb{R}^{k-1}$ the first element of which is proportional to $(\eta_2, \ldots, \eta_k)^T$. Since the $\boldsymbol{x}_j'$s are orthonormal, the proportionality constant is $\tilde{\eta} = \left(\sum_{j=2}^{k} \eta_j^2\right)^{-\frac{1}{2}}$. A symplectic orthogonal transformation for the $(2k-2)$-dimensional space $\operatorname{span}(\boldsymbol{x}_2', \ldots, \boldsymbol{x}_k', \boldsymbol{y}_2', \ldots, \boldsymbol{y}_k')$ is obtained imposing that the vectors $\boldsymbol{y}_j'$ undergo the same orthogonal transformation. This results in a passive transformation O_3 that only acts nontrivially on the last $k-1$ modes and can be grouped with O_2. Defining $\tilde{O}_2 = O_3 O_2$ we note that $\tilde{O}_2 K_1 = K_1 \tilde{O}_2$ since the two transformations act on different sets of modes. Reconstruction is then achieved acting a *single* controlled-Z between the first two modes

$$\tilde{K}_2 = \begin{pmatrix} & \mathbb{I}_k & & 0_k \\ 0 & \tilde{\eta}^{-1} & 0 & \ldots & \\ \tilde{\eta}^{-1} & 0 & 0 & \ldots & \mathbb{I}_k \\ \vdots & & \ddots & & \end{pmatrix}. \tag{B16}$$

The whole decoding corresponds then to the symplectic matrix

$$\tilde{S}_D^A = \tilde{K}_2 \tilde{O}_2 K_S K_1 O_1. \tag{B17}$$

Note that $\tilde{O}_2$ can be commuted through $K_S K_1$ and incorporated in O_1 to form a global passive transformation. All the squeezing required for the decoding is contained in $\tilde{K}_2 K_S K_1$ which acts trivially on all but the first two modes, and hence Bloch-Messiah factorization can be applied to factor it as a passive transformation, followed by two independent single-mode squeezers, followed by another passive transformation. In the end, this would lead to a decomposition

$$\tilde{S}_D^A = V_2 \Delta V_1 \tag{B18}$$

where V_1 is a passive transformation on all k modes, Δ consists of independent squeezers on the first two modes, and V_2 is a passive transformation on the first two modes.

Finally, we note that the number of squeezers can be further reduced to one by replacing the controlled-Z with a homodyne measurement on the second mode followed by a displacement on the first mode depending on the measurement outcome. Indeed, after $K_S O_2 K_1 O_1$ has been applied, the position quadrature of the first mode is already $\boldsymbol{x}\cdot\boldsymbol{\xi}^A$, whereas the momentum operator is $\boldsymbol{y}\cdot\boldsymbol{\xi}^A - \tilde{\eta}^{-1} q_2''$ where $q_2'' = \boldsymbol{x}_2''\cdot\boldsymbol{\xi}^A$ is the position quadrature of the second mode. If the latter is measured, e.g. by homodyne detection, the operator q_2'' is effectively replaced by a real number γ and the transformation $\boldsymbol{y}\cdot\boldsymbol{\xi}^A - \tilde{\eta}^{-1}\gamma \mapsto \boldsymbol{y}\cdot\boldsymbol{\xi}^A$ can be achieved by a displacement on the first mode.

2. Multi-mode secret state

In the case of a m-modes secret state, the matrix D has $2m$ rows and $2k$ columns, with k the number of players in the access party A. Recall that

$$D J^{(k)} D^T = J^{(m)} \tag{B19}$$

$$D\boldsymbol{\xi}^A = \boldsymbol{\xi}^{\mathrm{s}} + B\boldsymbol{p}^{\mathrm{sqz}}. \tag{B20}$$

The goal is again to extend the matrix D, adding $2k-2m$ rows, in such a way that the resulting matrix is symplectic and maps the quadratures of the first m modes of A to the secret quadratures, apart from distortions due to finitely-squeezed quadratures. In general the resulting matrix will involve squeezing. We aim at minimizing the number of squeezers. To this end, let us consider a matrix $\tilde{D}$, obtained by a partial extension of D, that is, $\tilde{D}$ is obtained adding $2l \leq 2k-2m$ to D in such a way that

$$\tilde{D} J^{(k)} \tilde{D}^T = J^{(m+l)}. \tag{B21}$$

If we manage to write $\tilde{D} = SV$ for some symplectic matrix $S \in \mathrm{Sp}(2m+2l, \mathbb{R})$ and V such that $VV^T = \mathbb{I}_{2m+2l}$, $V J^{(k+l)} V^T = J^{(m+l)}$ then decoding can be completed without adding more squeezers to those contained in S, the number of which is necessarily smaller than or equal to $m+l$ (as can be seen applying Bloch-Messiah factorization to S). In fact, $VV^T = \mathbb{I}_{2m+2l}$ means the rows of V are orthonormal, and since $\tilde{D} J^{(k)} \tilde{D}^T = J^{(m+l)}$, the orthogonal and symplectic complements of $\mathcal{V} \equiv \mathrm{span}\left(\left\{\tilde{D}(j)\right\}\right)$, where $\left\{\tilde{D}(j)\right\}$ denotes the rows of $\tilde{D}$, coincide $\mathcal{V}^J = \mathcal{V}^\perp$. We can thus find an orthonormal basis of $\mathcal{V}^J$ the elements of which are also orthogonal to each vector in $\mathcal{V}$ by the same procedure used in the previous subsection to construct an orthonormal basis of $\mathcal{V}_1$.

Let us now show that for a general D, at most $2m$ rows have to be added. Indeed $\Gamma = DD^T$ and $\Gamma' = \tilde{D}\tilde{D}^T$ are both symmetric, positive-definite matrices. apart from a possible rescaling, they are covariance matrices corresponding to physical states. Requiring that $\tilde{D} = SV$ and simultaneously $VV^T = \mathbb{I}_{2m+2l}$ implies

$$\Gamma' = SVV^T S^T = SS^T \tag{B22}$$

which means Γ' is proportional to the covariance matrix of a pure state. It follows that Γ' is (proportional to) a covariance matrix that purifies Γ. It is known that m ancillas are sufficient to purify a Gaussian state of m modes [23], so $l \leq m$. Since we have no *a priori* information about the structure of Γ, m ancillary modes are necessary in the worst case.

Suppose we compute S and V from the purification of DD^T. As anticipated, we can extend V to a symplectic orthogonal matrix O with the same procedure used in the previous subsection. We then extend S to a symplectic matrix $\tilde{S}$ that acts trivially on all but the first $2m$ modes. We can apply Bloch-Messiah reduction to $\tilde{S}$ and decompose it into a passive transformation that can be absorbed in O, a matrix K consisting of $2m$ independent squeezers on the first $2m$ modes, and a final passive transformation V acting on the first $2m$ modes, so in the end S_D^A has the form $S_D^A = VKO$.

Appendix C: Effect of finite-squeezing noise on the decoded state

We first show that for general input states the Wigner function of the reconstructed state can be represented as the Wigner function of the input state convoluted with a Gaussian filter function depending on the input squeezing. We then restrict to Gaussian secrets and derive the expression reported in Eq. (19) of the reconstruction fidelity for single mode, coherent input (secret) states.

1. General input states

We now show that for any input state ρ_{s}, with Wigner function $W_{\mathrm{s}}(\boldsymbol{\xi})$, not necessarily Gaussian, the Wigner function $W_{\mathrm{out}}(\boldsymbol{\xi})$ of the state reconstructed by an access party is given by a convolution of W_{s} with a Gaussian

filter function. This function is related to the input squeezing, the encoding S_L and the decoding S_D^A and becomes narrower for larger squeezing, eventually converging to a Dirac delta. In this limit, the convolution outputs exactly the secret Wigner function $W_{\rm s}$, meaning that the reconstruction is perfect.

Let us start from Eq. (13), which we recall here for convenience

$$\boldsymbol{\xi}^{\rm out} = B\boldsymbol{p}^{\rm sqz} + \boldsymbol{\xi}^{\rm s} \tag{C1}$$

where $\boldsymbol{\xi}^{\rm out} \equiv D\boldsymbol{\xi}^A$ as in the main text. If the matrix B were the zero matrix, then the outcomes of the measurement of any quadrature of the output state would follow the same probability distribution as if the same measurement had been performed on the input state. It follows that the output Wigner function $W_{\rm out}(\boldsymbol{\xi})$ would be equal to the input Wigner function $W_{\rm s}(\boldsymbol{\xi})$. If the matrix B is not zero, the output state is obtained by tracing out all squeezed modes. This amounts to averaging over all possible measurement outcomes for the squeezed quadratures $p_j^{\rm sqz}$. By assumption, the input modes are independently squeezed, so each $p_j^{\rm sqz}$ will contribute with a random shift distributed according to a Gaussian probability density with zero mean and variance $\sigma_j^2 = e^{-2r_j}/2$. Since the map that associates a Wigner function to each density matrix is linear, the output Wigner function is

$$\begin{aligned} W_{\rm out}(\boldsymbol{\xi}) &= \int \left(\prod_{j=1}^{n} \mathrm{d}y_j \frac{e^{-\frac{y_j^2}{2\sigma_j^2}}}{\sigma_j\sqrt{2\pi}} \right) W_{\rm in}(\boldsymbol{\xi} - B\boldsymbol{y}) \\ &= \frac{1}{\det\Delta\,(2\pi)^{\frac{n}{2}}} \int \mathrm{d}^n y \exp\left(-\frac{1}{2}\boldsymbol{y}^T\Delta^{-2}\boldsymbol{y}\right) W_{\rm in}(\boldsymbol{\xi} - B\boldsymbol{y}) \end{aligned} \tag{C2}$$

with $\Delta = \mathrm{diag}(\sigma_1, \ldots, \sigma_n)$. Eq. (C2) is valid for arbitrary input states. The case of a Gaussian $W_{\rm in}$ is discussed in the following.

2. Gaussian input states

Since the protocol only involves Gaussian (squeezed) ancillary states, Gaussian operations (passive interferometers, squeezers) and Gaussian measurement (homodyne), the procedure of encoding and then decoding can be described as a Gaussian channel. If the input states are also Gaussian, they are fully specified by the quadratures' mean values $\boldsymbol{\xi}_0$ and covariance matrix Γ

$$\begin{aligned} (\boldsymbol{\xi}_0)_j &= \langle \xi_j \rangle \\ \Gamma_{jl} &= \langle \{\xi_j, \xi_l\} \rangle. \end{aligned} \tag{C3}$$

The action of a Gaussian channel can then be described as [23]

$$\begin{cases} \boldsymbol{\xi}_0 \mapsto \mathcal{T}\boldsymbol{\xi}_0 + \boldsymbol{d} \\ \Gamma \mapsto \mathcal{T}\Gamma\mathcal{T}^T + \mathcal{N} \end{cases} \tag{C4}$$

where $\boldsymbol{d} \in \mathbb{R}^{2m}$, $\mathcal{T}$ and $\mathcal{N} = \mathcal{N}^T \geq 0$ are $2m \times 2m$ real matrices such that $\mathcal{N} + iJ^{(m)} - i\mathcal{T}J^{(m)}\mathcal{T}^T \geq 0$.

Let us focus on a single access party A. By construction, the quadratures of the reconstructed mode are related to the secret quadratures by Eq. (C1) (Eq. (13)). We directly see that $\mathcal{T} = \mathbb{I}$ and $\boldsymbol{d} = \boldsymbol{0}$. In order to characterize the channel defined by decoding and reconstruction by A we just need to find $\mathcal{N}$. This is easily accomplished remembering that the input squeezed and secret modes are not correlated, so that

$$\langle p_j^{\rm sqz} p_l^{\rm sqz} \rangle = \langle \xi_a^{\rm s} p_l^{\rm sqz} \rangle = 0 \tag{C5}$$

for any l, a and $j \neq l$, whence

$$\frac{1}{2}\langle \{\xi_a^{\rm out}, \xi_b^{\rm out}\} \rangle = \frac{1}{2}\sum_l B_{al}B_{bl}\Delta^2 p_l^{\rm sqz} + \frac{1}{2}\langle \{\xi_a^{\rm s}, \xi_b^{\rm s}\} \rangle. \tag{C6}$$

Denoting $\Delta^2 = \mathrm{Diag}\left(\Delta^2 p_1^{\rm sqz}, \ldots, \Delta^2 p_n^{\rm sqz}\right)$ and comparing with Eq. (C4) we arrive at

$$\mathcal{N} = B\Delta^2 B^T. \tag{C7}$$

For the rest of this section, we restrict for simplicity to the case where all the modes are squeezed by the same parameter r, so that

$$\mathcal{N} = \mathcal{N}(r) = \frac{e^{-2r}}{2} BB^T. \tag{C8}$$

Suppose furthermore that the secret is a single-mode coherent state $\rho_{\rm s} = |\alpha\rangle\langle\alpha|$, the covariance matrix of which is proportional to the 2×2 identity matrix $\Gamma = \mathbb{I}_2/2$. To compute the Fidelity $\mathcal{F}(\alpha, r)$ as a function of the squeezing parameter for an arbitrary input coherent state $|\alpha\rangle$ we use the fact that for a pure input state, the fidelity reduces to a trace, which is just an overlap integral, in our case between two Gaussian functions, in the Wigner function formalism [37]

$$\begin{aligned} \mathcal{F}(\alpha, r) &= \langle\alpha|\, \rho^{\rm out}(r)\, |\alpha\rangle \\ &= 2\pi \int \mathrm{d}q\ \mathrm{d}p\ W_\alpha(q,p)\, W_{\rm out}^{(r)}(q,p). \end{aligned} \tag{C9}$$

The Wigner functions of the two states are given by

$$W_{\alpha}\left(\boldsymbol{\xi}\right)=\frac{1}{\pi}\exp\left\{-\left(\boldsymbol{\xi}-\boldsymbol{\xi}_{0}\right)^{T}\left(\boldsymbol{\xi}-\boldsymbol{\xi}_{0}\right)\right\} \tag{C10}$$

$$W_{\mathrm{out}}^{(r)}\left(\boldsymbol{\xi}\right)=\frac{\det\left(\mathbb{I}+2\mathcal{N}\left(r\right)\right)^{-\frac{1}{2}}}{\pi}\exp\left\{-\left(\boldsymbol{\xi}-\boldsymbol{\xi}_{0}\right)^{T}\left(\mathbb{I}+2\mathcal{N}\left(r\right)\right)^{-1}\left(\boldsymbol{\xi}-\boldsymbol{\xi}_{0}\right)\right\} \tag{C11}$$

so that $\mathcal{F}\left(\alpha,r\right)$ reduces to the Gaussian integral

$$\mathcal{F}\left(\alpha,r\right)=\frac{2}{\pi}\det\left(\mathbb{I}+2\mathcal{N}\left(r\right)\right)^{-\frac{1}{2}}\int\mathrm{d}^{2}\boldsymbol{\xi}\exp\left\{-\boldsymbol{\xi}^{T}\left[\mathbb{I}+\left(\mathbb{I}+2\mathcal{N}\left(r\right)\right)^{-1}\right]\boldsymbol{\xi}\right\} \tag{C12}$$

where we used the fact that the integral does not change with the change of variable $\boldsymbol{\xi}\rightarrow\boldsymbol{\xi}+\boldsymbol{\xi}_{0}$. Standard integration techniques lead to

$$\begin{aligned}\mathcal{F}\left(\alpha,r\right)&=\frac{2}{\pi}2\pi\left[\det\left(\mathbb{I}+2\mathcal{N}\left(r\right)\right)\right]^{-\frac{1}{2}}\left\{\det\left[2\left(\mathbb{I}+\left(\mathbb{I}+2\mathcal{N}\left(r\right)\right)^{-1}\right)\right]\right\}^{-\frac{1}{2}}\\&=4\left[\det\left(\mathbb{I}+2\mathcal{N}\left(r\right)\right)\right]^{-\frac{1}{2}}\frac{1}{2}\left\{\det\left[\mathbb{I}+\left(\mathbb{I}+2\mathcal{N}\left(r\right)\right)^{-1}\right]\right\}^{-\frac{1}{2}}\\&=2\det\left\{\mathbb{I}+2\mathcal{N}\left(r\right)+\mathbb{I}\right\}^{-\frac{1}{2}}=\frac{1}{\sqrt{\det\left(\mathbb{I}+\mathcal{N}\left(r\right)\right)}}\end{aligned} \tag{C13}$$

where we used the fact that for a real number x and an $l\times l$ matrix M one has $\det\left(xM\right)=x^{l}\det\left(M\right)$ and Binet's formula to go from the second to the third line.

Now, by construction $\mathcal{N}\left(r\right)=\mathcal{N}\left(r\right)^{T}\geq0$ and $\mathcal{N}\left(r\right)\rightarrow0$ for $r\rightarrow\infty$, so $\mathcal{F}\left(\alpha,r\right)\rightarrow1$ for $r\rightarrow\infty$. Moreover, we can derive the simple expression of Eq. (19) by noting that there always exists an orthogonal matrix O such that $OBB^{T}O^{T}=\mathrm{diag}\left(\mu,\nu\right)$ and since the determinant and the trace are invariant under orthogonal transformations we have, after some algebra,

$$\begin{aligned}\det\left(\mathbb{I}+\mathcal{N}\left(r\right)\right)&=1+\frac{e^{-2r}}{2}\left(\mu+\nu\right)+\frac{e^{-4r}}{4}\mu\nu\\&=1+\frac{e^{-2r}}{2}\mathrm{Tr}\left(BB^{T}\right)+\frac{e^{-4r}}{4}\det\left(BB^{T}\right)\end{aligned} \tag{C14}$$

which plugged into Eq. (C13) leads to the desired expression.

Appendix D: Proof that the Haar measure of $\mathcal{B}$ is zero

We outline here a proof of the fact that the set $\mathcal{B}$ of matrices that cannot be used for secret sharing has zero Haar measure. We first note that integration with respect to the Haar measure of a function defined on $U\left(n\right)$ can be written as an ordinary integral over some real variables. We then recall a parametrization of $U\left(n\right)$ providing a realization of said variables. Finally, we conclude the proof linking the decodability conditions to the zero set of real analytic functions.

1. Haar measure in terms of real variables

Although the treatment could apply to more general situations, let us consider directly the case of $U\left(n\right)$. Since the unitary group is a real Lie group of dimension n^{2}, we can find an atlas, that is, a family of pairs $\left\{\left(V_{j},\gamma_{j}\right)\right\}$ such that the open sets $V_{j}\subseteq U\left(n\right)$ cover $U\left(n\right)$ and each map $\gamma_{j}:V_{j}\rightarrow\mathbb{R}^{n^{2}}$ is a homeomorphism. For any function f defined on $U\left(n\right)$ we can define a function g on $\mathcal{E}=\bigcup_{j}\gamma_{j}\left(V_{j}\right)\subseteq\mathbb{R}^{n^{2}}$ as

$$g\left(\boldsymbol{\lambda}\right)=f\left(\gamma_{j}^{-1}\left(\boldsymbol{\lambda}\right)\right) \tag{D1}$$

for all $\boldsymbol{\lambda}\in\mathcal{E}\cap\gamma_{j}\left(V_{j}\right)$. Using the theorem of change of variable, we can then find real valued functions $\Delta_{j}\left(\boldsymbol{\lambda}\right)$ such that we can write any integral with respect to the Haar measure, which we denote by $\mathrm{d}\mu^{H}$, as an integral over a region of $\mathbb{R}^{n^{2}}$

$$\int_{V_{j}}f\left(\alpha\right)\mathrm{d}\mu^{H}\left(\alpha\right)=\int_{\gamma_{j}\left(V_{j}\right)}f\left(\gamma_{j}^{-1}\left(\boldsymbol{\lambda}\right)\right)\Delta_{j}\left(\boldsymbol{\lambda}\right)\mathrm{d}^{n^{2}}\lambda. \tag{D2}$$

The integral over the whole unitary group can be defined appropriately gluing together the charts $\{(V_j, \gamma_j)\}$ [42].

2. Parametrization of $U(n)$

Instead of an atlas, we consider here a single chart which covers *almost all* of $U(n)$ (we will not prove this). This is sufficient for our goals.

In particular, we will consider the parametrization in terms of Euler angles that was used in [64] to numerically generate Haar distributed unitary matrices. It relies on the fact that any unitary matrix $\alpha \in U(n)$ can be obtained as the composition of rotations in two-dimensional subspaces. Each elementary rotation is represented by a $n \times n$ matrix $E^{(j,k)}$ the entries of which are all zero except for

$$\begin{aligned} E^{(j,k)}_{ll} &= 1 \quad \text{for } l = 1,\ 2,\ \ldots,\ n-1 \quad l \neq j,\ k \\ E^{(j,k)}_{jj} &= \cos(\phi_{jk})\, e^{i\psi_{jk}} \\ E^{(j,k)}_{jk} &= \sin(\phi_{jk})\, e^{i\chi_{jk}} \\ E^{(j,k)}_{kj} &= -\sin(\phi_{jk})\, e^{-i\chi_{jk}} \\ E^{(j,k)}_{kk} &= \cos(\phi_{jk})\, e^{-i\psi_{jk}} \end{aligned} \tag{D3}$$

From these elementary rotations one can construct the $n-1$ composite rotations

$$\begin{aligned} E_1 &= E^{(1,2)}(\phi_{12}, \psi_{12}, \chi_1) \\ E_2 &= E^{(2,3)}(\phi_{23}, \psi_{23}, 0)\, E^{(1,3)}(\phi_{13}, \psi_{13}, \chi_2) \\ E_3 &= E^{(3,4)}(\phi_{34}, \psi_{34}, 0)\, E^{(2,4)}(\phi_{24}, \psi_{24}, 0) \\ &\quad \times E^{(1,4)}(\phi_{14}, \psi_{14}, \chi_3) \\ &\vdots \\ E_{n-1} &= E^{(n-1,n)}(\phi_{n-1,n}, \psi_{n-1,n}, 0) \\ &\quad \times E^{(n-2,n)}(\phi_{n-2,n}, \psi_{n-2,n}, 0) \ldots \\ &\quad \times E^{(1,n)}(\phi_{1n}, \psi_{1n}, \chi_{n-1}) \end{aligned} \tag{D4}$$

and finally any matrix $\alpha \in U(n)$ can be written as

$$\alpha = e^{i\eta} E_1 E_2 \ldots E_{n-1}. \tag{D5}$$

This can be seen as a function defined in the region $\mathcal{E} \subset \mathbb{R}^{n^2}$ that takes n^2 angles

$$\begin{aligned} 0 \leq \phi_{jk} < \frac{\pi}{2} \text{ for } 1 \leq j < k \leq n, \\ 0 \leq \psi_{jk} < 2\pi \text{ for } 1 \leq j < k \leq n, \\ 0 \leq \chi_l < 2\pi \text{ for } 1 \leq l < n, \\ 0 \leq \eta < 2\pi \end{aligned} \tag{D6}$$

and outputs a $n \times n$ unitary matrix. In summary we defined a map $\gamma^{-1} : \mathcal{E} \to V \subset U(n)$ which is one-to-one and the image of which is the whole $U(n)$, except for a set of zero Haar measure. In practice, given any $\boldsymbol{\lambda} \in \mathcal{E}$ we can construct the matrix $\alpha = \gamma^{-1}(\boldsymbol{\lambda})$. So for any function $f : U(n) \to \mathbb{R}$ we can define $g : \mathbb{R}^{n^2} \to \mathbb{R}$ such that $g(\boldsymbol{\lambda}) = f\left(\gamma^{-1}(\boldsymbol{\lambda})\right)$. If f is measurable with respect to the Haar measure, we can write

$$\begin{aligned} \int_{U(n)} f(\alpha)\, \mathrm{d}\mu^H(\alpha) &= \int_V f(\alpha)\, \mathrm{d}\mu^H(\alpha) \\ &= \int_{\mathcal{E}} f\left(\gamma^{-1}(\boldsymbol{\lambda})\right) \Delta(\boldsymbol{\lambda})\, \mathrm{d}^{n^2}\lambda \end{aligned} \tag{D7}$$

with

$$\Delta(\boldsymbol{\lambda}) = \frac{1}{\prod_{k=1}^{n} \mathrm{Vol}\left(S^{2k-1}\right)} \left(\prod_{1 \leq j < k \leq n} \sin^{2j-1}(\phi_{jk}) \right) \tag{D8}$$

where $\mathrm{Vol}\left(S^{2k-1}\right)$ is the hypersurface of the $2k-1$ dimensional sphere in $2k$ dimensions [2], and

$$\mathrm{d}^{n^2}\lambda = \left(\prod_{1 \leq j < k \leq n} \mathrm{d}\phi_{jk} \right) \left(\prod_{1 \leq j < k \leq n} \mathrm{d}\psi_{jk} \right) \left(\prod_{1 \leq l < n} \mathrm{d}\chi_l \right) \mathrm{d}\eta. \tag{D9}$$

The normalization included in the function Δ ensures that

$$\int_V \mathrm{d}\mu^H(\alpha) = \int_{\mathcal{E}} \Delta(\boldsymbol{\lambda})\, \mathrm{d}^{n^2}\lambda = 1. \tag{D10}$$

Now, since $0 \leq \Delta(\boldsymbol{\lambda}) \leq 1\ \forall \boldsymbol{\lambda} \in \mathcal{E}$ we have

$$\begin{aligned} \int_{U(n)} f(\alpha)\, \mathrm{d}\mu^H(\alpha) &= \int_{\mathcal{E}} f\left(\gamma^{-1}(\boldsymbol{\lambda})\right) \Delta(\boldsymbol{\lambda})\, \mathrm{d}^{n^2}\lambda \\ &\leq \int_{\mathcal{E}} f\left(\gamma^{-1}(\boldsymbol{\lambda})\right) \mathrm{d}^{n^2}\lambda. \end{aligned} \tag{D11}$$

What we want to prove is that the integral of the indicator function $\mathbb{I}_{\mathcal{B}}$ of $\mathcal{B}$

$$\mathbb{I}_{\mathcal{B}}(\alpha) = \begin{cases} 1 & \alpha \in \mathcal{B} \\ 0 & \alpha \notin \mathcal{B} \end{cases} \tag{D12}$$

over $U(n)$ with respect to the Haar measure is equal to zero. This will be achieved if we manage to prove that

$$\int_{\mathcal{E}} \mathbb{I}_{\mathcal{B}}\left(\gamma^{-1}(\boldsymbol{\lambda})\right) \mathrm{d}^{n^2}x = 0 \tag{D13}$$

which is equivalent to

$$\int_{\gamma(\mathcal{B})} \mathrm{d}^{n^2}\lambda = 0 \tag{D14}$$

namely that the image of $\mathcal{B}$ under γ has zero measure in $\mathcal{E}$. This is proven in the next section leveraging the fact that through γ^{-1} the coefficients of any unitary matrix are written as real analytic functions of the angles.

---

[2] For example, for $k = 1$, $\mathrm{Vol}\left(S^{2k-1}\right) = 2\pi$ is the length of the circle in the plane.

3. Real analytic functions

Our main result then follows from the observation that $\mathcal{B}$ is the union of the zero sets of real analytic functions. Real analytic functions are defined analogously to their complex counterpart: a function $f : \mathbb{R}^N \to \mathbb{R}$ is analytic on an open set D if it can be represented as the sum of a converging power series in a neighbourhood of any point $x_0 \in D$ [43]. As in the complex case, a real analytic function is either identically zero, or its zero set has zero measure [43, 44] (See also [45] for a self-contained proof).

The parametrization of unitary matrices introduced in the previous subsection gives the coefficients of any unitary matrix as a product of trigonometric functions and complex exponentials of the angles. The coefficients of any symplectic orthogonal matrix are real or imaginary parts of a unitary matrix, so they are trigonometric functions of the angles. As it is well known, sine and cosine can always be written as power series. The set of real analytic functions $\mathcal{F}$ is closed under linear combinations with real coefficients and point-wise multiplication [3]. $\mathcal{F}$ is also closed under quotient as long as the denominator is not equal to zero [4]. The coefficients $(S_L)_{jl}(\boldsymbol{\lambda})$ are real analytic functions defined on $\mathcal{E}$. For each access party A, $\det\left(M\ H^A\right)$ is a polynomial in the entries of S_L and thus defines a real analytic function of the angles in $\mathcal{E}$. It follows that for all A, $\gamma^{-1}\left(\mathcal{B}^A\right)$ has zero Lebesgue measure on $\mathcal{E}$ This implies that the Haar measure of each $\mathcal{B}^A$ is zero. Positivity and countable additivity of the Haar measure imply $0 \leq \mu_H(\mathcal{B}) \leq \sum_A \mu_H\left(\mathcal{B}^A\right)$, so the Haar measure of $\mathcal{B}$ is also zero. This concludes the proof.

Appendix E: Interferometers for Fig. 2

We report here the X and Y blocks of the matrices S_L corresponding to the interferometers used for the plots in Fig. 2. apart from that used for Fig. 2a, the matrices were obtained choosing the interferometer that would lead to the lowest value of $\nu_{\max}$ out of 10^3 chosen from the Haar measure.

1. Fig. 2a

$$X = \begin{pmatrix} -0.293099 & -0.803506 & -0.311073 \\ 0.128259 & -0.376779 & 0.463209 \\ -0.633935 & -0.0662967 & 0.145639 \end{pmatrix} \quad Y = \begin{pmatrix} 0.0921935 & 0.16507 & 0.368724 \\ 0.650109 & -0.23828 & -0.384196 \\ -0.254222 & 0.352131 & -0.619594 \end{pmatrix} \tag{E1}$$

2. Fig. 2b

$$X = \begin{pmatrix} 0.596667 & 0.175214 & 0.100266 \\ 0.108915 & 0.458534 & -0.680759 \\ 0.426961 & -0.608681 & -0.134113 \end{pmatrix} \quad Y = \begin{pmatrix} -0.0698255 & 0.405573 & 0.658688 \\ -0.457902 & 0.174213 & -0.272814 \\ -0.485058 & -0.440131 & 0.0151496 \end{pmatrix} \tag{E2}$$

3. Fig. 2c

$$\begin{aligned} X &= \begin{pmatrix} 0.300365 & 0.29053 & -0.291467 & 0.497589 & -0.0499837 \\ 0.0193436 & -0.0889674 & -0.576899 & 0.216171 & -0.181089 \\ 0.068743 & -0.627185 & 0.0456175 & 0.267772 & 0.488823 \\ 0.313121 & -0.292716 & 0.202423 & -0.254404 & -0.472559 \\ 0.591341 & 0.0132897 & -0.118776 & -0.45464 & 0.0190248 \end{pmatrix} \\ Y &= \begin{pmatrix} 0.312353 & -0.285854 & 0.469979 & 0.285289 & -0.0937025 \\ 0.0839586 & -0.117954 & -0.320784 & -0.442078 & 0.509978 \\ 0.445916 & -0.00774418 & -0.243163 & 0.0854139 & -0.15446 \\ 0.382669 & 0.26366 & 0.163123 & 0.252382 & 0.425447 \\ -0.0840343 & -0.513083 & -0.339929 & 0.121405 & -0.16842 \end{pmatrix} \end{aligned} \tag{E3}$$

[3] If $f(x),\ g(x) \in \mathcal{F}$, then $h(x) = f(x)\, g(x) \in \mathcal{F}$.

[4] If $f(x),\ g(x) \in \mathcal{F}$, then the function h defined wherever f and g are both defined and $g(x) \neq 0$ as $h(x) = f(x)/g(x) \in \mathcal{F}$.

4. Fig. 2d

$$X = \begin{pmatrix} -0.17138 & 0.363352 & 0.220969 & 0.0345219 \\ 0.158628 & -0.268691 & 0.342882 & -0.0159773 \\ 0.478503 & -0.474253 & -0.255255 & 0.12308 \\ -0.435812 & -0.0371908 & 0.0669927 & -0.343434 \end{pmatrix}$$
$$Y = \begin{pmatrix} -0.529669 & -0.40525 & 0.435797 & 0.392287 \\ 0.460908 & 0.266619 & 0.628541 & 0.325934 \\ -0.130468 & -0.312016 & -0.235265 & 0.544141 \\ -0.128694 & 0.486635 & -0.351609 & 0.556099 \end{pmatrix} \tag{E4}$$

[1] W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).
[2] P. W. Shor, in *Proceedings of 37th Conference on Foundations of Computer Science* (1996) pp. 56–65.
[3] D. Gottesman, Phys. Rev. A **57**, 127 (1998).
[4] E. Knill, R. Laflamme, and W. H. Zurek, Science **279**, 342 (1998).
[5] C. H. Bennett and G. Brassard, Theoretical Computer Science **560**, 7 (2014), theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.
[6] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[7] S. Wiesner, SIGACT News **15**, 78 (1983).
[8] M. Hemmo and O. Shenker, Studies in History and Philosophy of Science Part B: Studies in History and Philosophy of Modern Physics **32**, 555 (2001), the Conceptual Foundations of Statistical Physics.
[9] S. Lloyd, Phys. Rev. A **56**, 3374 (1997).
[10] L. Viola, E. Knill, and S. Lloyd, Phys. Rev. Lett. **82**, 2417 (1999).
[11] L. Viola and S. Lloyd, Phys. Rev. A **58**, 2733 (1998).
[12] P. Hayden and J. Preskill, Journal of High Energy Physics **2007**, 120 (2007).
[13] K. Brádler and C. Adami, Phys. Rev. D **92**, 025030 (2015).
[14] P. Hayden, S. Nezami, G. Salton, and B. C. Sanders, New Journal of Physics **18**, 083043 (2016).
[15] M. Ahmadi, Y.-D. Wu, and B. C. Sanders, Phys. Rev. D **96**, 065018 (2017).
[16] Y.-D. Wu, A. Khalid, and B. C. Sanders, New Journal of Physics **20**, 063052 (2018).
[17] D. A. Lidar and T. A. Brun, *Quantum Error Correction* (Cambridge University Press, Cambridge, 2013).
[18] P. Hayden, P. W. Shor, and A. Winter, Open Systems & Information Dynamics **15**, 71 (2008).
[19] D. Gottesman, Phys. Rev. A **61**, 042311 (2000).
[20] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
[21] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
[22] M. Ben-Or, C. Crepeau, D. Gottesman, A. Hassidim, and A. Smith, in *2006 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS'06)* (2006) pp. 249–260.
[23] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
[24] T. Tyc and B. C. Sanders, Phys. Rev. A **65**, 042310 (2002).
[25] T. Tyc, D. J. Rowe, and B. C. Sanders, Journal of Physics A: Mathematical and General **36**, 7625 (2003).
[26] P. van Loock and D. Markham, AIP Conference Proceedings **1363**, 256 (2011).
[27] H.-K. Lau and C. Weedbrook, Phys. Rev. A **88**, 042313 (2013).
[28] J. Niset, U. L. Andersen, and N. J. Cerf, Phys. Rev. Lett. **101**, 130503 (2008).
[29] P. van Loock, Journal of Modern Optics **57**, 1965 (2010), https://doi.org/10.1080/09500340.2010.499047.
[30] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, Phys. Rev. Lett. **92**, 177903 (2004).
[31] S. Armstrong, M. Wang, R. Y. Teh, Q. Gong, Q. He, J. Janousek, H.-A. Bachor, M. D. Reid, and P. K. Lam, Nature Physics **11**, 167 EP (2015).
[32] Y. Cai, J. Roslund, G. Ferrini, F. Arzani, X. Xu, C. Fabre, and N. Treps, Nature Communications **8**, 15645.
[33] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).
[34] A. Ferraro, S. Olivares, and M. Paris, *Gaussian states in quantum information* (Bibliopolis, Naples, 2005).
[35] H.-A. Bachor and T. C. Ralph, *A guide to experiments in quantum optics* (Wiley, Weinheim, 2004).
[36] B. Dutta, N. Mukunda, and R. Simon, Pramana **45**, 471 (1995).
[37] U. Leonhardt, *Measuring the Quantum State of Light*, Cambridge Studies in Modern Optics (Cambridge University Press, Cambridge, 1997).
[38] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature **421**, 238 EP (2003).
[39] M. Gu, C. Weedbrook, N. C. Menicucci, T. C. Ralph, and P. van Loock, Phys. Rev. A **79**, 062318 (2009).
[40] U. Chabaud, T. Douce, F. Grosshans, E. Kashefi, and D. Markham, "Building trust for continuous variable quantum states," (2019), arXiv:1905.12700.
[41] A. Fasano and S. Marmi, *Analytical mechanics: an introduction* (Oxford University Press, Oxford, 2006).
[42] A. W. Knapp, *Lie groups beyond an introduction*, Vol. 140 (Birkhäuser, Boston, 2013).
[43] W. Rudin *et al.*, *Principles of mathematical analysis*, Vol. 3 (McGraw-hill, New York, 1964).
[44] S. G. Krantz and H. R. Parks, *A primer of real analytic functions* (Springer Science & Business Media, New York, 2002).

[45] B. Mityagin, "The zero set of a real analytic function," (2015), arXiv:1512.07276.
[46] F. Caruso, J. Eisert, V. Giovannetti, and A. S. Holevo, New Journal of Physics **10**, 083030 (2008).
[47] M. S. Kim and N. Imoto, Phys. Rev. A **52**, 2401 (1995).
[48] S. L. Braunstein and H. J. Kimble, Phys. Rev. Lett. **80**, 869 (1998).
[49] L.-M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **84**, 2722 (2000).
[50] R. Simon, Phys. Rev. Lett. **84**, 2726 (2000).
[51] N. J. Cerf, A. Ipe, and X. Rottenberg, Phys. Rev. Lett. **85**, 1754 (2000).
[52] F. Grosshans and P. Grangier, Phys. Rev. A **64**, 010301 (2001).
[53] H. Vahlbruch, M. Mehmet, K. Danzmann, and R. Schnabel, Phys. Rev. Lett. **117**, 110801 (2016).
[54] U. L. Andersen, T. Gehring, C. Marquardt, and G. Leuchs, Physica Scripta **91**, 053001 (2016).
[55] C. Jacquard, *A single-photon subtractor for spectrally multimode quantum states*, Phd thesis, Université Pierre et Marie Curie - Paris VI (2017).
[56] M. Habibidavijani and B. C. Sanders, "Continuous-variable ramp quantum secret sharing with gaussian states and operations," (2019), arXiv:1904.09506.
[57] A. Marin, D. Markham, and S. Perdrix, in *8th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2013)*, Leibniz International Proceedings in Informatics (LIPIcs), Vol. 22, edited by S. Severini and F. Brandao (Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, 2013) pp. 308–324.
[58] T. Morimae, Phys. Rev. Lett. **109**, 230502 (2012).
[59] K. Marshall, C. S. Jacobsen, C. Schäfermeier, T. Gehring, C. Weedbrook, and U. L. Andersen, Nature Communications **7**, 13795 EP (2016), article.
[60] R. Takagi and Q. Zhuang, Phys. Rev. A **97**, 062337 (2018).
[61] F. Albarelli, M. G. Genoni, M. G. A. Paris, and A. Ferraro, Phys. Rev. A **98**, 052350 (2018).
[62] A. Marin and D. Markham, Phys. Rev. A **88**, 042332 (2013).
[63] S. L. Braunstein, Phys. Rev. A **71**, 055801 (2005).
[64] K. Zyczkowski and M. Kus, Journal of Physics A: Mathematical and General **27**, 4235 (1994).