

# Boson Sampling in Low-depth Optical Systems

R. van der Meer,<sup>1,\*</sup> S. Huber,<sup>2</sup> P. W. H. Pinkse,<sup>1</sup> R. García-Patrón,<sup>3</sup> and J. J. Renema<sup>1</sup>

<sup>1</sup>*Adaptive Quantum Optics, MESA+ Institute for Nanotechnology, University of Twente, PO Box 217, 7500 AE Enschede, The Netherlands*

<sup>2</sup>*Leibniz Supercomputing Centre of the Bavarian Academy of Sciences and Humanities, Boltzmannstr. 1, 85748 Garching, Germany*

<sup>3</sup>*School of Informatics, University of Edinburgh, Edinburgh EH8 9AB, UK*

(Dated: October 12, 2021)

**Optical losses are the main obstacle to demonstrating a quantum advantage via boson sampling without leaving open the possibility of classical spoofing. We propose a method for generating low-depth optical circuits suitable for boson sampling with very high efficiencies. Our circuits require only a constant number of optical components (namely three) to implement an optical transformation suitable for demonstrating a quantum advantage. Consequently, our proposal has a constant optical loss regardless of the number of optical modes. We argue that sampling from our family of circuits is computationally hard by providing numerical evidence that our family of circuits converges to that of the original boson sampling proposal in the limit of large optical systems. Our work opens a new route to demonstrate an optical quantum advantage.**

Recently, the world has seen the first claims of a demonstration of a quantum advantage [1–4], i.e. the first systems in which a quantum computer outperforms a classical one at some specific, well-defined computational task. These systems represent a major milestone on the road toward applications of quantum computing for tasks beyond those that can be carried out with classical computers.

Boson sampling is a protocol to demonstrate a quantum advantage using quantum interference in linear optics [5]. In boson sampling,  $n$  indistinguishable photons are created at photon sources and sent through a linear optical network whose transformation matrix is chosen uniformly according to the Haar measure. The task is to generate samples from the output distribution of this interferometer when measured in the Fock basis. For a sufficiently large optical system, the probability distribution is given by permanents of matrices that are very well approximated by identical and independently distributed (i.i.d.) Gaussian elements. This distribution is believed to be hard to sample from for a classical computer, with the computational cost scaling as  $n2^n$  for the best-known classical algorithms [6], which places the boundary of a quantum advantage at  $n \approx 50$  photons [7]. At the same time, a linear optical network can natively implement this computational task through multi-photon interference and thereby generate samples from the target output distribution efficiently.

Since this protocol was proposed in 2011, there has been major progress on its experimental implementation. This started with smaller-scale boson sampling experiments [8–15] to the current state of the art experiments [16, 17], which consists of a 144 mode Gaussian boson sampler with 25 two-mode squeezed photon sources [3].

The challenge in carrying out these experiments is to adhere as closely as possible to the original boson

sampling protocol, and not introduce any imperfections, which may give rise to classical simulability. The general physical picture is that noise degrades the level of quantum interference in these systems, opening up the way for either a direct simulation [18–24], or spoofing a benchmark test [25, 26].

The strongest imperfection in large-scale boson sampling experiments is photon loss, which is an imperfection where not every photon that is generated in the sources ultimately results in a detection event in one of the detectors. For all proposed variants of boson sampling, loss is an imperfection that degrades the strength of quantum interference, although only for some variants it is known how to use this fact to construct an efficient classical simulation [22]. Finding ways of improving the optical transmission of boson sampling experiments is therefore an urgent problem. This is especially true since, in all current implementations of boson sampling, the number of optical components that must be traversed grows linearly with the width of the optical circuit, and hence the optical loss grows exponentially with the circuit size [27].

Another imperfection that plays a role in large-scale boson sampling experiments is detector blinding, which occurs when the number of modes  $m$  is comparable to the number of photons  $n$ , meaning that a significant fraction of photons will end up in identical output modes, which is termed a *collision*. In this situation, if threshold detectors are used at the outputs, some photons are not detected, which constitutes an imperfection that can be used for simulation [28]. In order to avoid collisions, the number of optical modes must scale as  $m \propto n^2$ , a scaling that is typically not obeyed in experiments [2, 3, 29].

In this work, we present a simultaneous solution to the problems of optical loss and detector blinding by proposing a constant-optical depth circuit that is scalable to the required thousands of optical modes. This circuit is realized in the form of a thin optical scatterer (e.g. a ground glass plate) placed in a  $4f$ -configuration in the simultaneous focal point of two lenses (see Fig. 1). We make use

---

\* r.vandermeer-1@utwente.nl

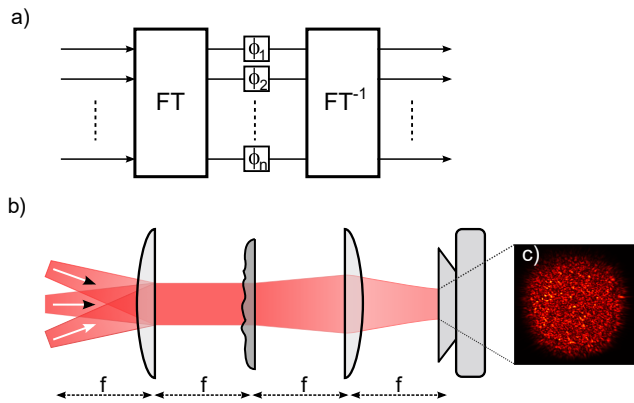


FIG. 1. A schematic of the proposed network with 4 input modes. a) The mathematical description of the physical apparatus as shown in b). The apparatus consists of two lenses and a thin, rough surface in between the lenses. The random interference pattern as observed on the detector (c) is known as speckle.

of the fact that a lens implements a Fourier transform on an almost arbitrary number of optical modes - up to 1 million modes per  $\text{mm}^2$  [30] - to conveniently realize a network with three components and constant optical loss in the system size. When a Fourier transform is implemented as pairwise mode interactions, e.g. in integrated optics, the number of required interactions per mode in the circuit scales as the logarithm of the number of modes involved. [31, 32]. We estimate that the overall efficiency of this protocol will be 85 – 90%, which would be sufficient to defeat all currently known classical simulation algorithms for boson sampling.

The price of this low-tech implementation is a complete loss of reconfigurability of the optical system. Furthermore, the fact that our scattering system scrambles the phase of each incoming  $k$ -vector in an identical way induces an additional constraint to the transmission matrix  $U$ , namely that it must be of *circulant* form, i.e. that each row of the sampling matrix is a copy of the previous row shifted by one entry. These additional correlations in the sampling matrix could *prima facie* affect the computational hardness of the protocol. The bulk of this work is concerned with presenting a combination of numerically and theoretical results which provide evidence that these additional correlations disappear in the appropriate limits of large numbers of photons and modes, thereby making our system suitable as a low-loss implementation of boson sampling. We name our proposal *circulant boson sampling* after the circulant nature of the scattering matrix.

Our work is organized as follows: we start in Section I with some physical arguments based on concepts from scattering theory. Then, Section. II formally introduces the circulant boson sampling and identifies the problems which need to be solved to guarantee the computational complexity. Section III gives an informal overview of the main results on demonstrating the computational complexity. Sections IV and V show the detailed results in

which we show how circulant boson sampling maintains computational complexity. Finally, Section VI addresses the technical feasibility of the system and focuses on the required hardware.

## I. THIN SCATTERING SYSTEMS

In this section, we will use some concepts from scattering theory to build up physical intuition for circulant boson sampling. For this, we start with a short description of thick scattering systems and then introduce the circulant network.

Perhaps counterintuitively, disorder is a desirable feature in many classical optical systems, where a high number of independent optical modes is needed. An example is in microscopy, where a diffusor is used to convert a point source into quasi-uniform illumination. Functionalizing disorder to achieve new optical applications is an active field of research [30, 33, 34].

A crucial factor that determines the properties of a scattering system is how often light is scattered while traversing the medium. Everyday optical systems in which scattering plays a role are typically multiple-scattering (‘thick’) systems, examples of which are white paint and milk. In multiple-scattering materials, incident light scatters many times on average before it diffuses out of the material. Repeated scattering events collectively scramble the polarization of the incoming light and effectively erase all directionality, i.e., the light is scattered in all  $4\pi$  directions. However, even in thick optical samples, the output distribution pattern is not uniform when pumped with coherent light. The random paths which the light takes through the sample are coherent and hence undergo interference. This random interference leads to a pattern of spatial intensity variations, which is referred to as speckle. An example of speckle is shown in Fig. 1b).

The properties of speckle patterns have been extensively studied [30, 35, 36]. A key property of speckle is its high degree of randomness. Random interference of many independent optical paths causes a complex Gaussian distribution of the elements of the scattering matrix. This is observed experimentally through the Rayleigh distribution of the optical field strengths leading to an exponential distribution of the intensities of the speckle pattern [35–37]. In the limit of thick optical systems, small submatrices of the scattering matrix approach an i.i.d. Gaussian distribution, as the scattering effectively erases all structure and only a part of all transmission modes can be observed. The fact that the matrix elements are i.i.d. Gaussian distributed turns out to be precisely the requirement for the computational complexity of boson sampling [5].

Unfortunately, boson sampling also requires a low-loss optical system, and for this, thick scattering systems are not suitable [38–40]. The ultimate reason for this is that in a multiple-scattering system the light is scattered over a  $4\pi$  solid angle, which makes a collection of all the light

scattered from the sample experimentally infeasible.

The network proposed in Fig. 1, which uses a single thin scattering layer, can be thought of as a system that combines the high degree of randomness of a thick scattering system with low optical loss. Such a system still grants access to a large number of modes, but at the same time reduces the losses since all the light will be transmitted over a small spread of spatial angles [36].

Unfortunately, having only one layer of scatterers does not allow for the same degree of mode mixing as is the case in thick scattering media. The consequence of this is that while the individual matrix elements in the scattering matrix all follow a Gaussian distribution (in the language of scattering theory ‘exhibit fully developed speckle’) [41], they exhibit significant correlations (in the language of scattering theory: they strongly exhibit a memory effect), and it is not given that the distribution of submatrices of such a matrix approaches an i.i.d. Gaussian distribution. It is precisely these additional circulant correlations that are the subject of this work.

## II. BOSON SAMPLING

In this section, we will first introduce boson sampling. Then, we will introduce a few key arguments from its original proposal [5] regarding the hardness of boson sampling, followed by our proposal for a modified protocol based on circulant matrices. A comprehensive and more in-depth discussion on boson sampling can be found in [42].

In a boson sampling experiment,  $n$  indistinguishable photons are injected in  $n$  distinct input modes of an  $m \times m$  random lossless interferometer ( $m > n$ ). The photons interfere as they propagate through the interferometer, resulting in an output probability distribution comprised of  $\binom{m+n-1}{n}$  entries.

Assume without loss of generality that the photons are incident on the first  $n$  input modes of the system, such that the input wave function is given by:

$$|\psi_{\text{in}}\rangle = |1\rangle^{\otimes n} |0\rangle^{\otimes m-n}, \quad (1)$$

and let the transmission through the interferometer be described by a complex unitary matrix  $U \in \mathbb{C}^{m \times m}$  drawn from the Haar measure. The output state is then given by:

$$|\Psi_{\text{out}}\rangle = \sum_{\mathbf{s}} P_{\mathbf{s}} |n_{o,1}^{(\mathbf{s})}, n_{o,2}^{(\mathbf{s})}, \dots, n_{o,m}^{(\mathbf{s})}\rangle, \quad (2)$$

with  $\mathbf{s}$  a particular output configuration and  $P_{\mathbf{s}}$  its corresponding probability amplitude [43]. Finally,  $n_{o,m}^{(\mathbf{s})}$  denotes the number of bosons in the output channel  $m$  given this configuration  $\mathbf{s}$ . The probability associated with a certain outcome  $P_{\mathbf{s}}$  is given by the interference of how the  $n$  input photons can end up at that specific output configuration  $\mathbf{s}$ . This is given by the permanent of an  $n \times n$  submatrix  $U_{\mathbf{T}}$  relating the used input modes to the

output configuration [5, 43]

$$P_{\mathbf{s}} = \frac{\text{perm}(U_{\mathbf{T}})}{\sqrt{n_{o,1}^{(\mathbf{s})}! \dots n_{o,m}^{(\mathbf{s})}!}}, \quad (3)$$

with the submatrix  $U_{\mathbf{T}} = U_{\rho,s}$ , with  $\rho$  the input configuration as defined in Eq. 1. The denominator is a normalization term and perm denotes the permanent. The permanent is defined as:

$$\text{perm}(U) = \sum_{\sigma \in S_n} \prod_{j=1}^n U_{j,\sigma(j)}, \quad (4)$$

with  $\sigma$  summing over the set of all permutations  $S_n$ .

The computational complexity of boson sampling ultimately derives from the conjecture that approximate sampling over the probability distribution given by  $|P_{\mathbf{s}}|^2$  is computationally hard, if  $U_{\mathbf{T}}$  is given by a matrix of i.i.d. Gaussian entries. The intuition behind the choice of this family of matrices is that i.i.d. Gaussian matrices have no internal structure which a classical algorithm could exploit to achieve a speedup.

For the matrices  $U_{\mathbf{T}}$  to be close to i.i.d. Gaussian, two conditions must hold. First, any  $n$ -by- $n$  submatrix of  $U$  must converge to a matrix of i.i.d. Gaussians in the limit of a large number of modes. The intuition here is that as the submatrix becomes smaller with respect to the overall matrix  $U$ , the unitary constraint becomes less dominant, removing any correlations between the matrix elements. Aaronson and Arkhipov were able to show that if  $U$  is drawn uniformly according to the Haar measure, then for a scaling of  $m \propto n^5 \log n$ , an  $n$ -by- $n$  submatrix is close to i.i.d. Gaussian.

The second requirement is that the output distribution must actually be made up of  $n$ -by- $n$  matrices drawn from  $U$ , avoiding repeated rows or columns in  $U_{\mathbf{T}}$ . These arise when photons emerge from the same optical mode, which is termed a *collision*. The probability of collisions must be made arbitrarily small, a condition which is satisfied for Haar-random matrices when  $m \propto n^2$ .

To argue the hardness of our proposed protocol, we must show that these two conditions hold (perhaps with different polynomial scaling in the number of modes) for our proposed family of sampling matrices. Our goal in what follows will be to provide evidence that the intuition from sampling over Haar-random matrices holds also for circulant matrices, namely that the additional correlations which are introduced by the constraints on the matrices decay when the number of modes is made large enough with respect to the number of photons.

In our protocol, the only change we make compared to the original proposal [5] is the family of optical circuits over which we sample. Instead of Haar-random matrices, we now sample over matrices of the form  $U_c = F\Phi F^{-1}$ , where  $F$  is an  $n$ -by- $n$  Fourier matrix with the appropriate normalization and  $\Phi$  is a diagonal matrix whose entries are given by  $\Phi_{jj} = \exp(i\phi_j)$ , with each  $\phi_j$  chosen independently on the interval  $[0, 2\pi]$ . The resulting matrix

has the form:

$$U_c = \begin{bmatrix} c_1 & c_2 & \dots & c_m \\ c_m & c_1 & \dots & c_{m-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_2 & \dots & \dots & c_1 \end{bmatrix}, \quad (5)$$

with  $c_j \in \mathbb{C}$ , and is called a circulant matrix. Note that this matrix has only  $m$  unique elements since each row or column is a repetition of the previous one where all elements have been shifted by one position. These additional correlations are an additional obstacle in letting the elements of a truncated matrix  $U_T$  approach i.i.d. Gaussians.

### III. OVERVIEW OF RESULTS

In this section, we provide a general overview of our results. Our strategy to argue the computational complexity of circulant boson sampling is to closely follow the proof for standard boson sampling [5]. To this end, we must show that (1) truncations of circulant matrices should approach i.i.d. Gaussians with polynomial scaling in  $n$  and  $m$  and (2) that there is a polynomial scaling between  $n$  and  $m$  in which the no-collision condition holds. In this section we provide an informal overview of the main results on these two points. For both points, we rely on a combination of numerical and analytic results to provide our evidence.

A crucial fact about our system is that the output configurations are not equiprobable, unlike the Haar-random case [44]. This is due to the fact that repeated entries in the sampling matrix give rise to higher order moments of matrix elements in the expected value of the permanent. This fact means that the symmetry arguments employed in [5, 44] are not available to us.

**Truncations - analytical result** We show that the variation distance  $\Delta_C$  between the probability distribution of submatrices of circulants and the i.i.d. Gaussian ensemble is upper bounded by

$$\Delta_C \leq \dot{C} \frac{n^2}{\sqrt{m}} \quad (6)$$

For some universal constant  $\dot{C} > 0$ .

**Truncations - numerical results** We provide evidence that the eigenvalue spectrum of a truncated circulant matrix strongly resembles that of a truncated Haar-random matrix. In particular, we provide numerical evidence that the fidelity between the eigenvalue distribution of a Gaussian and truncated circulant matrix remains constant at  $m \propto n$  scaling.

Furthermore, we provide evidence that the convergence of permanents of truncated circulant matrices to permanents of i.i.d. Gaussian matrices have the same scaling as the convergence of permanents of truncated Haar matrices to permanents of i.i.d. Gaussian matrices. This is another, independent piece of evidence for the convergence of submatrices of circulant matrices to i.i.d. Gaussians.

**No collisions - Analytical results** Collisions in the matrix elements reduce the computational complexity of boson sampling. The original proposal uses Haar-random matrices, where every photon ‘blocks off’ a single potential output mode for the remaining photons (namely the one which it occupies). In circulant boson sampling, the cyclic nature of circulant matrices means that each photon blocks off  $n$  adjacent modes as well.

We show that if we assume all outcomes in the boson sampler are equiprobable averaged over all circulant matrices (which is only approximately true for circulant matrices), a scaling of  $m \propto n^3$  is required to achieve a constant probability of an outcome with repeated elements in the matrix (i.e. a collision).

**No collisions - numerical results** We use a Monte Carlo simulation to provide evidence that the  $m \propto n^3$  scaling inferred from our simplified calculation assuming equiprobable outcomes also holds when we take into account the fact that not all outcomes are equiprobable.

### IV. TRUNCATIONS APPROACH I.I.D. GAUSSIAN

In this section, we provide evidence that sufficiently small truncations of circulant matrices become close, in variation distance, to a matrix with i.i.d. Gaussian elements. To this end, we follow the strategy of the original boson sampling proposal [5]. Their approach has two steps. Firstly, they showed that a polynomially small submatrix of a larger, Haar-random unitary matrix becomes approximately Gaussian distributed. Then this result was used to prove the stronger statement, namely the multiplicative bound

$$p_S(X) \leq (1 + O(\delta))p_G(X), \quad (7)$$

$\forall X \in C^{n \times n}$  and with  $p_S$  and  $p_G$  the probability density functions of Haar random unitaries and i.i.d. Gaussians, respectively.

In the following subsections, we will first show that the submatrix of a circulant matrix approaches the i.i.d. Gaussian ensemble additively. Unfortunately, we were unable to prove the multiplicative bound from the additive bound. As additional evidence of convergence, we study both the eigenvalue spectra of truncated circulant matrices and the average outcome of permanents of truncated circulant matrices. Both approaches independently provide insight to the convergence to i.i.d. Gaussians.

#### A. Analytical results

We first present our analytical results providing evidence that the distribution of  $n$ -by- $n$  submatrices of non-identical elements (i.e. without repetitions in the elements) converges to an i.i.d. Gaussian distribution.

Rather than looking at a submatrix, we can limit ourselves to a single vector containing all elements of the submatrix. The vector has a length of  $d = m^2$  and thus

corresponds to the submatrix. The goal is to show that the effect of the unitary constraint on this vector becomes negligible for some suitable scaling of the length of the vector. For this first step, we use theorem 1.1 of [45].

**Theorem 1.** *Let  $\mathfrak{R}^d$  be a real Euclidian  $d$ -dimensional space of vectors  $x = (x_1, \dots, x_d)$  with the norm  $\|x\|_2^2 = \sum_{i=1}^d x_i^2$  and the scalar product  $\langle x, x \rangle = \|x\|_2^2$ . Let  $X_1, \dots, X_n$  be independent random vectors with a common mean  $E(X) = 0$ . Write  $S = \sum_{j=0}^n X_j$ . Throughout we assume that  $S$  has a degenerated distribution in the sense that the covariance operator, say  $\Sigma = \text{Cov}(S)$ , is invertible. Let  $Z \sim N(0, \Sigma)$  be a Gaussian random vector with the same covariance matrix  $S$ . Let  $C$  be the class of all convex subsets of  $\mathfrak{R}^d$ . Then there exists a universal constant  $C > 0$  such that*

$$\begin{aligned} \Delta_C &:= \sup_{A \in C} |Pr\{S \in A\} - Pr\{Z \in A\}| \\ &\leq Cd^{\frac{1}{4}} \sum_{j=1}^n E(\|\Sigma^{-\frac{1}{2}} X_j\|_2^3), \end{aligned} \quad (8)$$

where  $\Sigma^{-\frac{1}{2}}$  stands for the positive root of  $\Sigma$ .

We now show how we can apply this Theorem to the case where we pick  $d$  elements of a vector of length  $n$  which is the Fourier transform of a vector of random phases. Let  $\Phi_1, \dots, \Phi_m$  be i.i.d. uniform on  $[0, 2\pi]$ . Fix  $k_1, \dots, k_n \in \{1, \dots, m\}$ . For  $j = 0, \dots, m-1$ , define  $X_j^{(n)}$  to be the vector containing all matrix elements

$$\begin{aligned} X_j^{(n)} &= \frac{1}{\sqrt{n}} \begin{bmatrix} w_n^{jk_1} e^{i\phi_j} \\ \vdots \\ w_n^{jk_d} e^{i\phi_j} \end{bmatrix} \\ &= \frac{1}{n} \begin{bmatrix} \cos(\phi_j + 2\pi \frac{jk_1}{n}) \\ \sin(\phi_j + 2\pi \frac{jk_1}{n}) \\ \cos(\phi_j + 2\pi \frac{jk_2}{n}) \\ \vdots \\ \sin(\phi_j + 2\pi \frac{jk_n}{n}) \end{bmatrix} \in \mathfrak{R}^{2d}, \end{aligned} \quad (9)$$

where the first line is a column vector whose elements are given by a discrete Fourier transform applied on the vector of phases  $\phi_j$ , and  $w_n^{jk_l} = \frac{1}{\sqrt{n}} \exp(-\frac{2\pi i}{m} k_l j)$ . The second line expands the space by a factor two by splitting up the real and imaginary part of the previous line.

The  $X_j^{(n)}$  are independent and clearly,  $E(X_j^{(n)}) = 0$  for all  $j = 0, \dots, n-1$ . Furthermore, it can be checked that (under some assumptions on  $k_1, \dots, k_d$ , see [46])

$$\text{Cov}(\sum_{j=0}^{n-1} X_j^{(n)}) = \frac{1}{2} I_{2d}. \quad (10)$$

This covariance matrix is clearly invertible, hence we can

apply Theorem 1 to obtain:

$$\begin{aligned} \Delta_C &\leq Cd^{\frac{1}{4}} \sum_{j=0}^{n-1} E(\|(\frac{1}{2} I_{2n})^{-\frac{1}{2}} X_j^{(n)}\|_2^3) \\ &= 2^{\frac{3}{2}} Cd^{\frac{1}{4}} \sum_{j=0}^{n-1} E(\|X_j^{(n)}\|_2^3) \\ &= 2^{\frac{3}{2}} Cd^{\frac{1}{4}} \sum_{j=0}^{n-1} E\left(\sqrt{\frac{1}{n} \sum_{l=1}^d \cos^2(\phi_j + 2\pi \frac{jk_l}{n}) + \sin^2(\phi_j + 2\pi \frac{jk_l}{n})}\right)^3 \\ &= 2^{\frac{3}{2}} Cd^{\frac{1}{4}} \sum_{j=0}^{n-1} E\left(\frac{n^{\frac{3}{2}}}{d^{\frac{3}{2}}}\right) = 2^{\frac{3}{2}} Cd^{\frac{1}{4}} n^{-\frac{1}{2}} \\ &\leq \hat{C} \frac{d^2}{\sqrt{n}}. \end{aligned} \quad (11)$$

For a universal constant  $\hat{C} > 0$ . In other words, the unitary constraint is upper bounded by  $\frac{d^2}{\sqrt{n}}$ .

This result gives evidence that the number of modes must scale as  $m \propto n^4$  to hide the unitary constraint. This shows the submatrix-of-circulant approaches the i.i.d. Gaussian ensemble additively. Unfortunately, unlike the case of Haar-random matrices, there appears to be no easy way to use the additive bound to prove the multiplicative bound.

## B. Eigenvalue spectra

In the original boson sampling proposal, the multiplicative bound was found by examining the eigenvalue spectra. [47–50]. Inspired by this, we carry out a Monte-Carlo simulation of the eigenvalue spectra. To this end,  $10^6$  truncated matrices of size  $n$ -by- $n$  are obtained, each from another Haar-random unitary and circulant unitary matrix of size  $m$ -by- $m$ . Each truncation is chosen such that repeated entries are absent, i.e., it implicitly assumes an outcome without collisions. To quantify the similarity of the two distributions  $A$  and  $B$ , we use the fidelity as given by: [51]

$$F(A, B) = \sum_{j=1}^n \sqrt{P(A)_j P(B)_j}, \quad (12)$$

where  $P(X)_j$  denotes the probability of the  $j^{\text{th}}$  eigenvalue. Note that this Monte-Carlo approach can only provide insights to the average fidelity between the eigenvalue spectra, it does not lower-bound the minimum fidelity.

We start with a system of fixed photon number  $n = 3$ , where we show how the fidelity of truncations of both Haar-random unitaries as well as circulant matrices with the i.i.d. Gaussian ensemble approach unity as the number of modes is increased. Figure 2a) shows how the

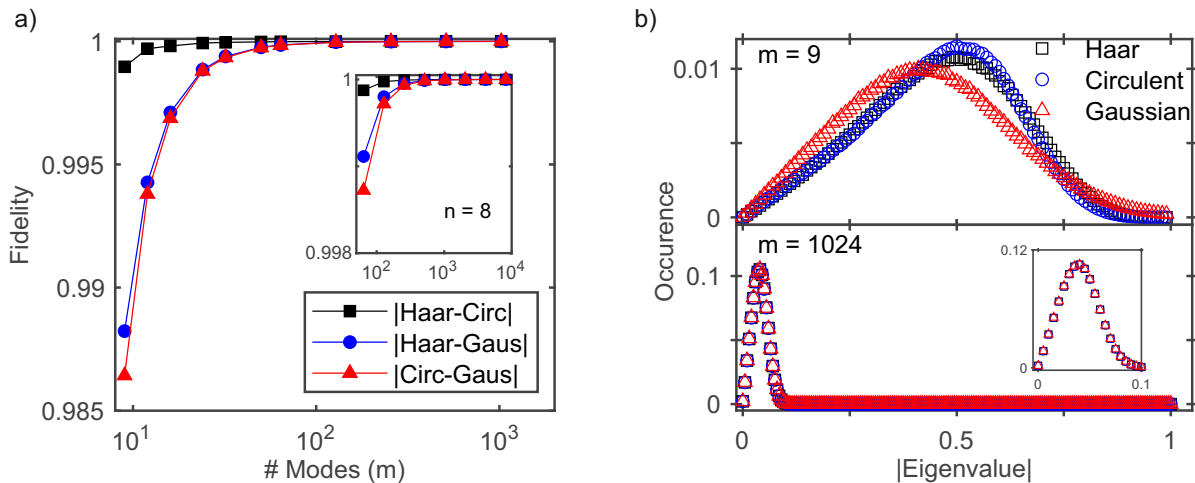


FIG. 2. a) The convergence of the fidelity between eigenvalue distributions in the case of 3 photons. The inset shows the case for 8 photons. b) Two examples of the eigenvalue distribution for 3 photons when  $m = 9$  and  $m = 1024$ . The inset on the bottom right is a zoom-in on the peak of the latter.

fidelity depends on the number of modes  $m$  at a fixed photon number. Despite the differences between the truncated-Haar and truncated-circulant matrix ensembles, it is striking how similar their approach to  $F = 1$  is as the number of modes is increased. That the distributions are indeed close is confirmed by the black points in Fig. 2a), which show the fidelity between the Haar and circulant distributions, which show that they resemble each other more than that either resembles the i.i.d. Gaussian ensemble. The inset shows that this behavior remains when the number of photons is increased, in this case to  $n = 8$ . The similarity of the fidelities as shown in 2a) is illustrated by the two example eigenvalue distributions shown in Fig. 2b). Again, the truncations of both the Haar-random and the circulant matrix are similar and in the limit of  $m \gg n$  clearly converge to that of i.i.d. Gaussians.

So far, we have considered eigenvalue distributions of truncated matrices at a fixed number of photons  $n$  as a function of the number of modes. The next thing to show is how the ratio of modes and photons should scale for a fixed fidelity. This is shown in Fig. 3, where the convergence of the fidelity between the circulant and Gaussian truncation is plotted as a function of the number of modes  $m$  for a different number of photons  $n$ . The x-axis is rescaled by the number of photons in order to emphasize the similar trend of the fidelity for all photons. The graph suggests that the number of modes should scale as  $m \propto n$ , however, note that this is the result after averaging over the space of circulant matrices; it is not the worst-case scenario. The deviation from the dashed line for a small number of photons is the result of using a finite number of samples in the simulation. This effect is more profound for small  $n$  as each random matrix only contributes  $n$  eigenvalues to the histogram.

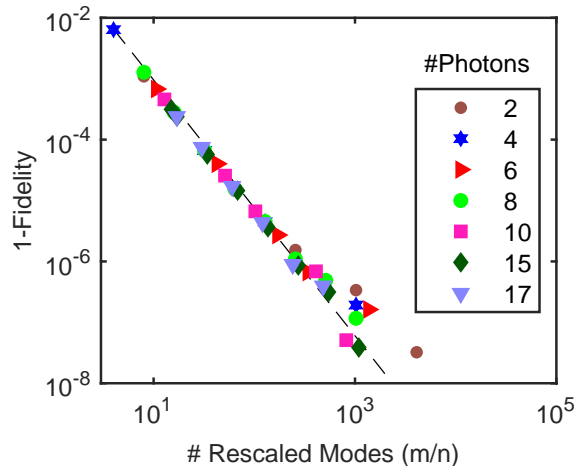


FIG. 3. Convergence of the fidelity between circulant and Gaussian truncations with a rescaled x-axis. The dashed line is a guide to the eye.

### C. Permanents

Another, more direct way to investigate the effect of the circulant correlations on the convergence to i.i.d. Gaussians is to look at the average outcome of permanents of submatrices of Haar-random and circulant matrices. If the correlations disappear with some suitable scaling of the number of modes and photons, the expected value of the permanent of a submatrix of a circulant  $C$  must approach that of the i.i.d. Gaussian ensemble  $X$ , which has  $E(|\text{Perm}(X)|^2) = n!/m^n$ . Having the average outcome of a permanent of a submatrix of a circulant matrix approach this value is a necessary but not a sufficient condition for the ensemble to approach that of i.i.d. Gaussians, but it can serve to provide numerical evidence.

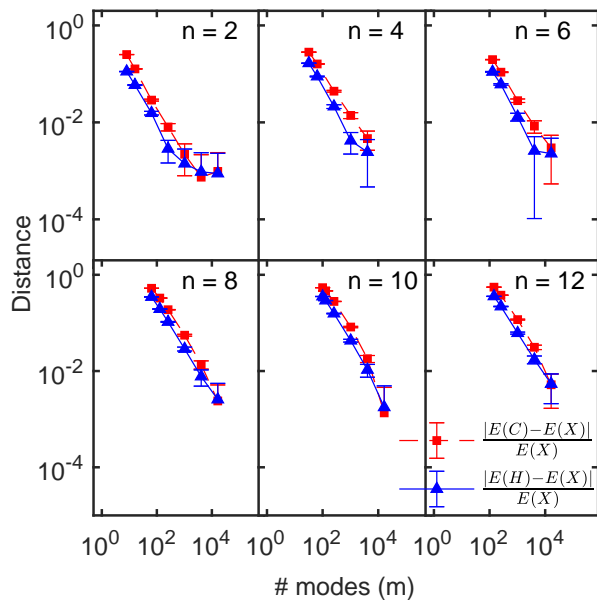


FIG. 4. Numerical evidence for the convergence of the average permanent for a various number of photons  $n$  as a function of the number of modes  $m$ . The red squares show how the distance between the average permanent of truncated circulant matrices and the result of i.i.d. Gaussian matrices diminishes with  $m$  and the blue triangles show the same for truncated Haar matrices.

Figure 4 shows how the distance between the expectation values of truncations of both a Haar-random unitary and a circulant unitary with the result of an i.i.d. Gaussian scale with the number of modes,  $m$ . Each data point is the mean of  $10^6$  random instances and the error bars denote the standard deviation. What is notable is that for each data point where we have sufficient numerical resolution in our simulation (as indicated by the error bars), the distance between Haar and Gaussian and between circulant and Gaussian differs only by a constant value as the number of modes is increased.

This result reinforces the picture from our study of the eigenvalue spectrum, namely that the submatrix-of-circulant distribution strongly resembles the submatrix-of-Haar distribution, which is known to converge to i.i.d. Gaussian in the appropriate limits. A full proof would require a multiplicative version of the result of section IV A.

## V. NO-COLLISIONS

The second prerequisite for our protocol is to show that the probability of observing collisions (i.e. outcomes with repeated matrix elements) becomes small with appropriate scaling of the number of modes  $m$  versus the number of photons  $n$ . In the case of a Haar-random matrix, this can be done fairly straightforwardly, because each outcome, regardless of collisions, is equiprobable [44]. This reduces the problem to a matter of combinatorics, namely

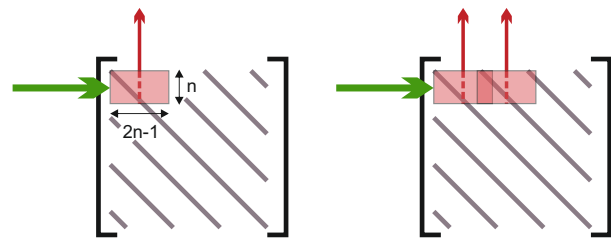


FIG. 5. Illustration of the counting argument where we assume an input (green) where photons enter in the first  $n$  modes. If one of these photons comes out of, for example, output mode  $n$  (red) then the other photons cannot get out of the first  $2n - 1$  output modes. (Left) The red block indicates what output modes are not allowed by 1 photon leaving. (Right) The forbidden regions by two photons may overlap, as long as the used output modes (dashed lines) do not enter the forbidden region of the other photons.

of counting the number of desired (no-collision) outcomes versus the number of total outcomes.

Unfortunately, for a circulant matrix, even in the limit where all elements are i.i.d. Gaussian, the outcomes are not on average equiprobable. The reason for this is that adjacent rows have repeated elements (see Fig. 5). These repeated elements have two consequences: first, they have the effect that any outcome where two photons are detected  $n$  modes apart will have repeated entries in its corresponding matrix  $U_T$ , meaning that it will certainly not be i.i.d. Secondly, an elementary calculation shows that these repeated elements cause higher-order moments of Gaussians to appear in the calculation, which affect the expected value, making some outcomes more likely than others.

To investigate the scaling of the no-collision condition with the number of photons and the number of modes, we follow the intuition of the previous section and make use of the fact that we have observed that the permanents of submatrices of circulant matrices without repeated elements resemble submatrices of Haar-random matrices in their behavior. We will start with a simple counting argument to find an analytical expression for the fraction of desired outcomes. Then we follow this up with numerical simulations to show that the intuition derived from this argument is correct.

### A. Number of good outcomes

The number of desired outcomes, i.e., without circulant correlations, can be found by a counting argument. For now, we assume for simplicity that all outcomes are equiprobable. To show this counting argument, assume without loss of generality that the photons are incident on the first  $n$  modes of the network. Each photon blocks exactly  $2n - 1$  output modes: on both sides of the output mode the first  $n - 1$  adjacent modes are not allowed since they contain the same value in the matrix and an



other +1 because a photon also blocks the its own output mode. See Fig. 5 for a schematic representation. These blocked regions may overlap, as long as none of the output modes are in these regions. Hence, in this limit, the fraction of good outcomes is given by:

$$N_{\text{good}} = \frac{m!_{2n-1}/(m-2n^2+n_{2n-1})}{\binom{m+n-1}{n}}, \quad (13)$$

where the subscripts denotes the  $x^{\text{th}}$  multifactorial, i.e.  $n!_x = n(n-x)(n-2x)(n-3x)\dots$ . Working out these terms and only taking the first two leading terms ( $n^k$  and  $n^{k-1}$ ) in both the numerator and denominator results in:

$$\begin{aligned} N_{\text{good}} &= \frac{m(m-2n+1)(m-4n+2)(m-6n+2)\dots}{(m+n-1)(m+n-2)(m+n-3)\dots} \\ &\approx \frac{m^n - m^{n-1} \sum_{j=0}^{n-1} j(2n-1)}{m^n + m^{n-1} \sum_{j=0}^{n-1} (n-j)} \\ &\approx \frac{m^n - \frac{1}{2}(n-1)(n-2)(2n-1)m^{n-1}}{m^n + \frac{1}{2}(n+1)nm^{n-1}} \\ &\approx \frac{m^n - n^3 m^{n-1}}{m^n + n^2 m^{n-1}}. \end{aligned} \quad (14)$$

Here the standard series  $\sum_{j=0}^{j=n} n = n \frac{n-1}{2}$  has been used. As we are interested in the regime  $m \gg n$ , we can rewrite it as a Laurent series at  $m = \infty$ :

$$\begin{aligned} N_{\text{good}} &\approx \frac{1 - n^3/m}{1 + n^2/m} \\ &= 1 - \sum_{j=1}^{\infty} (-1)^j \frac{n^{2j}(n+1)}{m^j} \\ &\approx 1 - \frac{n^3 + n^2}{m} + \mathcal{O}\left(\frac{n^5}{m^2}\right). \end{aligned} \quad (15)$$

This shows that the number of modes required to make the number of good (uncorrelated) outcomes dominate the experiment scales as  $m \propto n^3$ . The  $n^3$  scaling is only a small increase from the normal  $m \propto n^2$  scaling to hide the collisions. This is remarkable because there are additional correlations present in the circulant matrix and that a circulant matrix only has  $n$ , not  $n^2$  unique elements.

## B. Numerical results

The above derived scaling for the fraction of possible outcomes without circulant correlations can be verified numerically. Figure 6a) shows a Monte-Carlo simulation on how the fraction of correlated outcomes becomes small for some selected number of photons. Each data point is the average of  $5 \cdot 10^6$  samples, all drawn from independent instances of circulant unitaries. The error bars denote the standard deviation corresponding to a Bernoulli distribution. Each data set has a dashed line indicating the predicted  $\frac{1}{n^3}$  scaling. The figure hints at a  $m \propto n^3$  scaling, where the deviation for small photon

numbers can be understood as finite size effects and the fact that no uncorrelated output states are possible when  $m = n^2$ . These results confirm the scaling as predicted by the combinatorics of section V A.

The next step to show no-collisions is to identify the probability of ending up with an uncorrelated outcome and to show that this approaches 1 by increasing the total network size  $m$ . Therefore we first identify the number of uncorrelated (good) outcomes, just as in Fig. 6a, and then multiply that with the average probability associated with these good outcomes.

Figure 6b) shows how the probability of obtaining a correlated outcome scales with the number of photons and the number of modes. Each data point is the product of the fraction of good outcomes, similar to Fig. 6a), and the corresponding average probability of such outcome. Each sample is drawn from a circulant unitary and hence incorporates the unitary constraint. Note that this is a more stringent scenario than derived above in section V A. The error bars denote the standard deviation, where again a Bernoulli distribution is used to estimate the uncertainty in  $N_{\text{good}}$ . For each dataset -number of photons-, there is a dashed line indicating the predicted  $m \propto n^3$  scaling.

## VI. REQUIRED HARDWARE

In this section, we comment on the availability of the hardware needed to implement our proposal.

A key experimental advantage of our proposal is that it removes the need for fiber-coupled single-photon sources. For example, in photon sources based on parametric down-conversion, a key source of optical loss is the coupling from the photons into an optical fiber. In our protocol, the photon sources could directly illuminate the scatterer, removing the need for fiber coupling and its associated optical loss.

To implement the random phases, there are three natural candidates: ground glass plates, holographic plates, or spatial light modulators. The first candidate for implementing such random phases, would be a surface scatterer such as a ground glass plate. This naturally implements the phases by random height differences on the surface, which corresponds to a relative phase delay. The second method is to use a holographic plate, made of glass or polymer where the thickness varies throughout the plate. By varying the thickness of the object locally, the light picks up a relative phase depending on the thickness. This method also gives a fixed phase shift, but allows for some degree of design. The transmission of a ground glass plate or a holographic plate is limited by the impedance mismatch between the material used and air, resulting in reflection losses of a few percent of the light. The third method is a fully tunable version of a phase-plate: a phase-only spatial light modulator (SLM). A phase-only SLM typically consists of an LCD screen in which every pixel can give a variable delay to the incident light on that pixel, implementing a phase



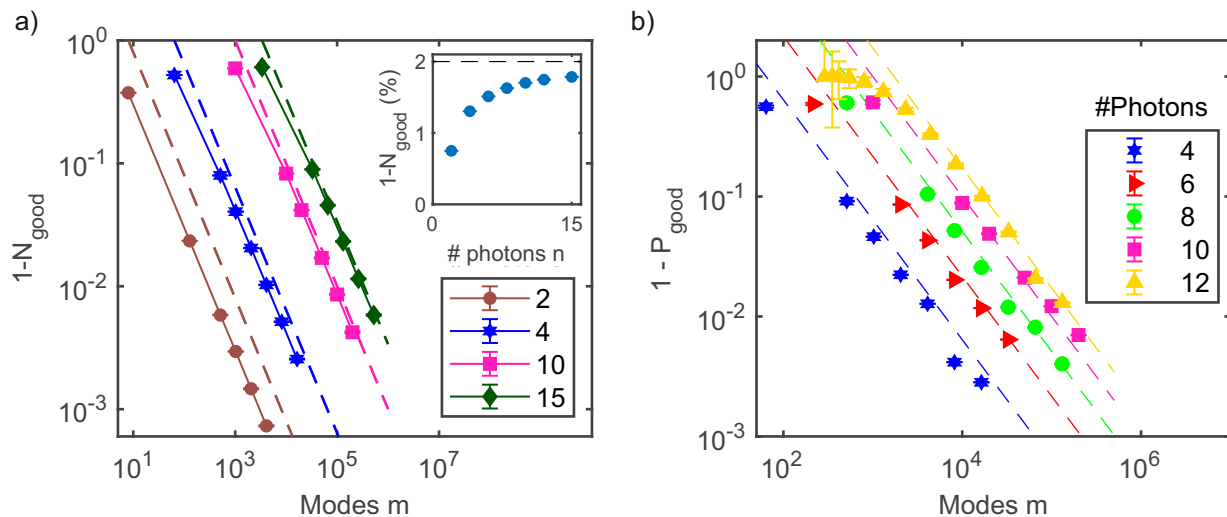


FIG. 6. a) Monte-Carlo calculation of good outcomes for a selected number of photons. The dashed line is the predicted scaling. Note that the numerical results approach the theory for a large number of photons. Inset: the convergence to the fraction predicted by the combinatorics (dashed line) at  $m/n^3 = 50$ . b) Monte-Carlo calculation of the number of good outcomes, multiplied with the average probability of a good outcome. The error bars denote the standard deviation of  $P_{\text{good}}$ . The dashed lines are guides to the eye showing the  $\propto n^3 m^{-1}$  scaling.

shift. As SLMs are versatile and induce low losses -up to 90% transmission efficiency-, SLMs are widely used in scattering adaptive-optics research [30].

Once the photons went through the optical network, they must be detected. For this, a single-photon sensitive camera is needed as the multi-photon interference manifests itself in the transverse plane. Since lumping different output modes together will result in decoherence of the interference pattern, the total number of modes from in the network must be smaller or equal to that of the detector, and each detector pixel should correspond with a diffraction-limited spot. Hence circulant boson sampling requires megapixel single-photon cameras, which is the major technological limitation of our protocol.

Superconducting nanowire single-photon detectors (SNSPD)s are a promising technology for such detectors. SNSPDs are reported to have record-high detection efficiencies [52, 53] for a single detection pixel. Currently SNSPD based cameras are being developed and up to 64 pixels are already reported on a regular basis [54–62]. The first kilopixel detector is already reported as well [63], and current electronics architecture is known to allow up to  $225 \times 225$  pixels [64]. The detection efficiency of these devices is limited by the low fill factor on the sensor, typically  $\approx 30\%$  and relative low quantum efficiency, which is typically in the order of  $\approx 30 - 40\%$ . It is estimated that the fill factor, however, can be improved

to  $\approx 90\%$  with already existing technology [63]. Furthermore, the detection efficiency can be improved greatly by also placing each of the detection pixels inside an optical cavity. Note that this is the default method to boost detection efficiencies close to 100% in single-pixel SNSPDs [53].

## VII. CONCLUSION

In conclusion, we have described and theoretically analysed a free-space optical method for implementing random matrices suitable for boson sampling in a way that induces only minimal loss while making many optical modes accessible. We anticipate that this method will be useful for high-optical transmission quantum advantage demonstrations in photonics.

## ACKNOWLEDGMENTS

RvdM and PWHP acknowledges funding from the Dutch Research Council (NWO) via QuantERA QUOMPLEX (Grant No. 680.91.037), and the Dutch Research Council (NWO), Veni programme 'Photonic Quantum Simulation', grant nr. 016.Veni.192.121. Furthermore we thank Peter Drummond for discussions.

[1] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth,

E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M. P. Harrigan, M. J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T. S. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang,

- D. Kafri, K. Kechedzhi, J. Kelly, P. V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandrà, J. R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michielsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Y. Niu, E. Ostby, A. Petukhov, J. C. Platt, C. Quintana, E. G. Rieffel, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, K. J. Sung, M. D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven, and J. M. Martinis, *Nature*, **1** (2019).
- [2] H.-S. Zhong, H. Wang, Y.-H. Deng, M.-C. Chen, L.-C. Peng, Y.-H. Luo, J. Qin, D. Wu, X. Ding, Y. Hu, P. Hu, X.-Y. Yang, W.-J. Zhang, H. Li, Y. Li, X. Jiang, L. Gan, G. Yang, L. You, Z. Wang, L. Li, N.-L. Liu, C.-Y. Lu, and J.-W. Pan, *Science* (2020), 10.1126/science.abe8770.
- [3] H.-S. Zhong, Y.-H. Deng, J. Qin, H. Wang, M.-C. Chen, L.-C. Peng, Y.-H. Luo, D. Wu, S.-Q. Gong, H. Su, Y. Hu, P. Hu, X.-Y. Yang, W.-J. Zhang, H. Li, Y. Li, X. Jiang, L. Gan, G. Yang, L. You, Z. Wang, L. Li, N.-L. Liu, J. Renema, C.-Y. Lu, and J.-W. Pan, arXiv:2106.15534 [physics, physics:quant-ph] (2021), arXiv:2106.15534 [physics, physics:quant-ph].
- [4] Y. Wu, W.-S. Bao, S. Cao, F. Chen, M.-C. Chen, X. Chen, T.-H. Chung, H. Deng, Y. Du, D. Fan, M. Gong, C. Guo, C. Guo, S. Guo, L. Han, L. Hong, H.-L. Huang, Y.-H. Huo, L. Li, N. Li, S. Li, Y. Li, F. Liang, C. Lin, J. Lin, H. Qian, D. Qiao, H. Rong, H. Su, L. Sun, L. Wang, S. Wang, D. Wu, Y. Xu, K. Yan, W. Yang, Y. Yang, Y. Ye, J. Yin, C. Ying, J. Yu, C. Zha, C. Zhang, H. Zhang, K. Zhang, Y. Zhang, H. Zhao, Y. Zhao, L. Zhou, Q. Zhu, C.-Y. Lu, C.-Z. Peng, X. Zhu, and J.-W. Pan, arXiv:2106.14734 [quant-ph] (2021), arXiv:2106.14734 [quant-ph].
- [5] S. Aaronson and A. Arkhipov, *Theory Comput.* **9**, 143 (2013).
- [6] H. J. Ryser, *Combinatorial Mathematics (Carus Mathematical Monographs No. 14)* (Mathematical Assn of Amer, 1963).
- [7] J. Wu, Y. Liu, B. Zhang, X. Jin, Y. Wang, H. Wang, and X. Yang, *National Science Review* **5**, 715 (2018), arXiv:1606.05836.
- [8] J. B. Spring, B. J. Metcalf, P. C. Humphreys, W. S. Kolthammer, X.-M. Jin, M. Barbieri, A. Datta, N. Thomas-Peter, N. K. Langford, D. Kundys, J. C. Gates, B. J. Smith, P. G. R. Smith, and I. A. Walmsley, *Science* **339**, 798 (2013).
- [9] M. A. Broome, A. Fedrizzi, S. Rahimi-Keshari, J. Dove, S. Aaronson, T. C. Ralph, and A. G. White, *Science* **339**, 794 (2013).
- [10] M. Tillmann, B. Dakić, R. Heilmann, S. Nolte, A. Szameit, and P. Walther, *Nat. Photonics* **7**, 540 (2013).
- [11] A. Crespi, R. Osellame, R. Ramponi, D. J. Brod, E. F. Galvão, N. Spagnolo, C. Vitelli, E. Maiorino, P. Mataloni, and F. Sciarrino, *Nat. Photonics* **7**, 545 (2013).
- [12] J. C. Loredo, M. A. Broome, P. Hilaire, O. Gazzano, I. Sagnes, A. Lemaitre, M. P. Almeida, P. Senellart, and A. G. White, *Phys. Rev. Lett.* **118**, 130503 (2017).
- [13] H. Wang, J. Qin, X. Ding, M.-C. Chen, S. Chen, X. You, Y.-M. He, X. Jiang, L. You, Z. Wang, C. Schneider, J. J. Renema, S. Höfling, C.-Y. Lu, and J.-W. Pan, *Phys. Rev. Lett.* **123**, 250503 (2019).
- [14] Y. He, X. Ding, Z.-E. Su, H.-L. Huang, J. Qin, C. Wang, S. Unsleber, C. Chen, H. Wang, Y.-M. He, X.-L. Wang, W.-J. Zhang, S.-J. Chen, C. Schneider, M. Kamp, L.-X. You, Z. Wang, S. Höfling, C.-Y. Lu, and J.-W. Pan, *Phys. Rev. Lett.* **118**, 190501 (2017).
- [15] H.-S. Zhong, Y. Li, W. Li, L.-C. Peng, Z.-E. Su, Y. Hu, Y.-M. He, X. Ding, W. Zhang, H. Li, L. Zhang, Z. Wang, L. You, X.-L. Wang, X. Jiang, L. Li, Y.-A. Chen, N.-L. Liu, C.-Y. Lu, and J.-W. Pan, *Phys. Rev. Lett.* **121**, 250505 (2018).
- [16] A. P. Lund, A. Laing, S. Rahimi-Keshari, T. Rudolph, J. L. O'Brien, and T. C. Ralph, *Phys. Rev. Lett.* **113**, 100502 (2014).
- [17] C. S. Hamilton, R. Kruse, L. Sansoni, S. Barkhofen, C. Silberhorn, and I. Jex, *Phys. Rev. Lett.* **119**, 170501 (2017).
- [18] J. J. Renema, A. Menssen, W. R. Clements, G. Triginer, W. S. Kolthammer, and I. A. Walmsley, *Phys. Rev. Lett.* **120**, 220502 (2018).
- [19] J. Renema, V. Shchesnovich, and R. Garcia-Patron, arXiv:1809.01953 [cond-mat, physics:physics, physics:quant-ph] (2018), arXiv:1809.01953 [cond-mat, physics:physics, physics:quant-ph].
- [20] R. García-Patrón, J. J. Renema, and V. Shchesnovich, *Quantum* **3**, 169 (2019), arXiv:1712.10037.
- [21] D. J. Brod and M. Oszmaniec, *Quantum* **4**, 267 (2020), arXiv:1906.06696.
- [22] J. J. Renema, *Phys. Rev. A* **101**, 063840 (2020).
- [23] B. Villalonga, M. Y. Niu, L. Li, H. Neven, J. C. Platt, V. N. Smelyanskiy, and S. Boixo, (2021), arXiv:2109.11525.
- [24] J. Shi and T. Byrnes, arXiv:2105.09583 [quant-ph] (2021), arXiv:2105.09583 [quant-ph].
- [25] F. Pan and P. Zhang, arXiv:2103.03074 [physics, physics:quant-ph] (2021), arXiv:2103.03074 [physics, physics:quant-ph].
- [26] J. F. F. Bulmer, B. A. Bell, R. S. Chadwick, A. E. Jones, D. Moise, A. Rigazzi, J. Thorbecke, U.-U. Haus, T. Van Vaerenbergh, R. B. Patel, I. A. Walmsley, and A. Laing, arXiv:2108.01622 [quant-ph] (2021), arXiv:2108.01622 [quant-ph].
- [27] R. García-Patrón, J. J. Renema, and V. Shchesnovich, *Quantum* **3**, 169 (2019).
- [28] A. S. Popova and A. N. Rubtsov, arXiv:2106.01445 [quant-ph] (2021), arXiv:2106.01445 [quant-ph].
- [29] V. S. Shchesnovich, *Int. J. Quantum Inform.* **18**, 2050044 (2020).
- [30] A. P. Mosk, A. Lagendijk, G. Leroosey, and M. Fink, *Nat Photon* **6**, 283 (2012).
- [31] R. Barak and Y. Ben-Aryeh, *J. Opt. Soc. Am. B* **24**, 231 (2007).
- [32] A. Crespi, R. Osellame, R. Ramponi, M. Bentivegna, F. Flamini, N. Spagnolo, N. Viggianiello, L. Innocenti, P. Mataloni, and F. Sciarrino, *Nat Commun* **7**, 10469 (2016).
- [33] I. M. Vellekoop and A. P. Mosk, *Opt. Lett.* **32**, 2309 (2007).
- [34] S. Rotter and S. Gigan, *Rev. Mod. Phys.* **89**, 015005 (2017).
- [35] C. W. J. Beenakker, arXiv:0904.1432 [cond-mat, physics:physics] (2009), arXiv:0904.1432 [cond-mat, physics:physics].
- [36] J. Goodman, *Speckle Phenomena in Optics: Theory and Applications* (Roberts & Company, 2007).
- [37] H. Di Lorenzo Pires, J. Woudenberg, and M. P. van Exter, *Phys. Rev. A* **85**, 033807 (2012).
- [38] H. Defienne, M. Barbieri, B. Chalopin, B. Chatel, I. A. Walmsley, B. J. Smith, and S. Gigan, *Optics Letters* **39**,

- 6090 (2014).
- [39] T. J. Huisman, S. R. Huisman, A. P. Mosk, and P. W. H. Pinkse, *Appl. Phys. B* **116**, 603 (2014).
- [40] T. A. W. Wolterink, R. Uppu, G. Ctistis, W. L. Vos, K.-J. Boller, and P. W. H. Pinkse, *Phys. Rev. A* **93**, 053817 (2016).
- [41] W. H. Peeters, J. J. D. Moerman, and M. P. van Exter, *Phys. Rev. Lett.* **104**, 173601 (2010).
- [42] D. J. Brod, E. F. Galvão, A. Crespi, R. Osellame, N. Spagnolo, and F. Sciarrino, *AP* **1**, 034001 (2019).
- [43] S. Scheel, arXiv:quant-ph/0406127 (2004), arXiv:quant-ph/0406127.
- [44] A. Arkhipov and G. Kuperberg, *Geom. Topol. Monogr.* **18**, 1 (2012).
- [45] V. Bentkus, *Theory Probab. Appl.* **49**, 311 (2005).
- [46] M. W. Meckes, *Some Results on Random Circulant Matrices* (Institute of Mathematical Statistics, 2009) pp. 213–223.
- [47] C. Mastrodonato and R. Tumulka, *Lett Math Phys* **82**, 51 (2007).
- [48] D. Petz and J. Réffy, *Periodica Mathematica Hungarica* **49**, 103 (2005).
- [49] D. Petz and J. Réffy, *Probab. Theory Relat. Fields* **133**, 175 (2005).
- [50] J. Réffy, *Asymptotics of Random Unitaries*, Ph.D. thesis, Budapest University of Technology and Economics, Budapest (2005).
- [51] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, 2010).
- [52] A. E. Lita, A. J. Miller, and S. W. Nam, *Opt. Express* **16**, 3032 (2008).
- [53] D. V. Reddy, D. V. Reddy, A. E. Lita, S. W. Nam, R. P. Mirin, and V. B. Verma, in *Rochester Conference on Coherence and Quantum Optics (CQO-11) (2019)*, Paper W2B.2 (Optical Society of America, 2019) p. W2B.2.
- [54] S. Doerner, A. Kuzmin, S. Wuensch, I. Charaev, F. Boes, T. Zwick, and M. Siegel, *Appl. Phys. Lett.* **111**, 032603 (2017).
- [55] A. Gaggero, F. Martini, F. Mattioli, F. Chiarello, R. Cernansky, A. Politi, and R. Leoni, *Optica, OPTICA* **6**, 823 (2019).
- [56] S. Miki, T. Yamashita, Z. Wang, and H. Terai, *Opt. Express, OE* **22**, 7811 (2014).
- [57] S. Miyajima, M. Yabuno, S. Miki, T. Yamashita, and H. Terai, *Opt. Express, OE* **26**, 29045 (2018).
- [58] A. K. Sinclair, E. Schroeder, D. Zhu, M. Colangelo, J. Glasby, P. D. Mauskopf, H. Mani, and K. K. Berggren, *IEEE Transactions on Applied Superconductivity* **29**, 1 (2019).
- [59] Q. Zhao, A. McCaughan, F. Bellei, F. Najafi, D. De Fazio, A. Dane, Y. Ivry, and K. K. Berggren, *Appl. Phys. Lett.* **103**, 142602 (2013).
- [60] Q.-Y. Zhao, D. Zhu, N. Calandri, A. E. Dane, A. N. McCaughan, F. Bellei, H.-Z. Wang, D. F. Santavicca, and K. K. Berggren, *Nature Photonics* **11**, 247 (2017).
- [61] D. Zhu, Q.-Y. Zhao, H. Choi, T.-J. Lu, A. E. Dane, D. Englund, and K. K. Berggren, *Nature Nanotechnology* **13**, 596 (2018).
- [62] J. P. Allmaras, E. E. Wollman, A. D. Beyer, R. M. Briggs, B. A. Korzh, B. Bumble, and M. D. Shaw, *Nano Letters* **20**, 2163 (2020).
- [63] E. E. Wollman, E. E. Wollman, V. B. Verma, V. B. Verma, A. E. Lita, W. H. Farr, M. D. Shaw, R. P. Mirin, and S. W. Nam, *Opt. Express, OE* **27**, 35279 (2019).
- [64] M. S. Allman, V. B. Verma, M. Stevens, T. Gerrits, R. D. Horansky, A. E. Lita, F. Marsili, A. Beyer, M. D. Shaw, D. Kumor, R. Mirin, and S. W. Nam, *Appl. Phys. Lett.* **106**, 192601 (2015).