Boson-Sampling: Progress, Challenges, and Opportunities Beyond Quantum Supremacy

Matthew Yeh
Electrical Engineering and Computer Sciences,
University of California, Berkeley, CA 94720

(Dated: May 8, 2020)

Boson-sampling is a nonuniversal model of quantum computation which finds its origins in linear optical quantum computing (LOQC). The problem involves sampling from the output distribution of n indistinguishable noninteracting bosons injected into an m-mode linear interferometer. This sampling problem is expected to be classically hard to simulate, making boson-sampling a strong candidate for demonstrating quantum supremacy in the near-term due to the relative simplicity of its experimental implementation. Given the context of Google's recent claim of quantum supremacy, the usefulness of boson-sampling has been called into question. In this paper, we provide an overview of recent progress in the field of boson-sampling, with a specific focus on its photonic implementation. We argue that boson-sampling can find application in numerous fields beyond its original context.

I. INTRODUCTION

Quantum information science has captured much interest from the scientific community in the past years, due its prospects for secure communications and exponential speedup over classical computers in solving certain problems [1]. As the nature of light is inherently quantum, it is no wonder that using photons as qubits, the fundamental unit of quantum information, has been an appealing route. The computational basis states $|0\rangle$, $|1\rangle$ can be encoded in various ways, e.g. using horizontal/vertical polarization or vacuum/single-photon Fock states. Moreover, single-qubit gates can be easily implemented using appropriate beam-splitters and phase-shifters.

However, as noted by DiVincenzo in 2000, one criteria for a scalable universal quantum computer is the ability to apply a universal set of quantum gates [2]. From an experimentalist's point of view, this essentially amounts to 1) arbitrary single-qubit rotations, and 2) a two-qubit entangling operation, such as the CNOT gate. So while single-qubit rotations are well within the reach of linear optics interferometers, the capability of such elements to perform two-qubit gates, and thus universal quantum computing, was under debate for many years.

It thus came as a well-received breakthrough when in 2001 Knill, Laflamme & Milburn (KLM) presented their celebrated theorem for Linear Optics Quantum Computing (LOQC) [3]. Under their approach, the application of certain gates are conditioned on feedforward measurements of ancillary photons, introducing an effective nonlinearity (using only linear optical elements) that can be exploited to provide a universal gate set. As with all candidate platforms for quantum computing, this is difficult to implement in practice, requiring a long list of experimental details and precise engineering. Universal LOQC thereby remains a long-term research goal.

It is from this context of LOQC that the boson-sampling problem arises. Aaronson & Arkhipov (AA) considered the intermediate problem of sampling from the output distribution of a passive linear optics network (i.e. no feedforward measurements) with Fock state inputs [4]. Surprisingly, they found strong evidence that this cannot be simulated efficiently on a classical computer for moderate photon numbers. This makes boson-sampling an attractive candidate for demonstrating quantum supremacy – the short-term goal of having a quantum computer solve a well-defined problem that no classical device, using the fastest methods, can solve in a reasonable amount of time [5]. In particular, boson-sampling provides certain advantages over more archetypal proposals, such as quantum simulation or a demonstration of Shor's algorithm for factoring integers. First, it solves a well-defined computational problem that can be *proven*, under reasonable complexity theory assumptions, to be classically intractable. Second, due to the relative simplicity of the experimental setup compared to a full-scale universal quantum computer, it has greater potential to be implemented in the near-term.

In this paper, we discuss recent advances in the field of boson-sampling, with a specific focus on its photonic implementation. We first provide a brief theoretical overview of the physical model, and establish the computational complexity of the problem. We then consider progress and challenges in the physical implementation of the experiment. Finally, in the context of Google's recent claim of quantum supremacy using a programmable superconducting processor [5], we explore how the field can progress beyond its origin in quantum supremacy. We argue that outside its original context, there remain many applications that can harness the unique properties of boson-sampling.

II. THEORETICAL OVERVIEW OF BOSON-SAMPLING

A. Physical Model

As the name suggests, the boson-sampling problem is in general well-defined for any situation where indis-

tinguishable noninteracting bosons interfere according to the evolution of a linear network, described by a random unitary matrix chosen according to the Haar measure [4]. However, for consistency and to maintain focus on the photonic implementation, we will describe the problem in the language of quantum optics. Figure 1 contains a schematic illustration of the boson-sampling problem.

We first begin by preparing n identical single photons in m modes. As in the original AA formulation, we typically consider $n \leq m \leq poly(n)$. Each mode has an associated creation operator $\hat{a}_i^\dagger$, which follows the standard bosonic commutation relations. Then, our input state can be described by:

$$\begin{aligned} |\psi_{in}\rangle &= |1_1 \dots 1_n 0_{n+1} \dots 0_m\rangle \\ &= \hat{a}_1^\dagger \dots \hat{a}_n^\dagger \, |0_1 \dots 0_m\rangle \end{aligned} \tag{1}$$

Without loss of generality, we have assumed that the n single photons are populating the first n modes. The bosons are then injected into an m-mode interferometer comprised of beamsplitters and phase-shifters that act on at most two modes at a time.

Let us consider these optical elements in more detail. According to the reciprocity relations [6], the unitary transformation corresponding to a beamsplitter $B(\theta, \phi)$ can be described by the 2×2 matrix

$$B(\theta, \phi) = \begin{bmatrix} \cos\theta & -e^{i\phi}\sin\theta \\ e^{-i\phi}\sin\theta & \cos\theta \end{bmatrix} \tag{2}$$

and for a phase-shifter, by

$$P(\phi) = \begin{bmatrix} e^{i\phi} & 0 \\ 0 & 1 \end{bmatrix}. \tag{3}$$

It is then straightforward to see that these two passive optical elements can generate all 2×2 unitaries. If we consider that we actually have m modes, we note that on the $m-2$ other modes that are not of interest, these elements simply act as the identity. These results can be generalized to state that all $m \times m$ unitaries U can be decomposed into a product of optical elements $U_1 \dots U_k$, each acting nontrivially on at most two modes [7]. Moreover, this can be done with $k = O(m^2)$ optical elements.

Thus, under the action of the interferometer, the creation operators evolve under the unitary transformation

$$\hat{a}_i^\dagger \to \sum_{j=1}^{m} U_{ij} \hat{a}_j^\dagger. \tag{4}$$

Throughout these measurements, the total photon number is preserved. Correspondingly, the output is a superposition of photon configurations $|S\rangle = |s_1 \dots s_m\rangle$, where $s_i \geq 0 \; \forall i$ and $\sum_{i=1}^m = n$. That is,

$$|\psi_{out}\rangle = \sum_S \alpha_S \, |S\rangle \, . \tag{5}$$

Finally, photon-number distinguishing photodetectors are used to measure every output port. It can be shown

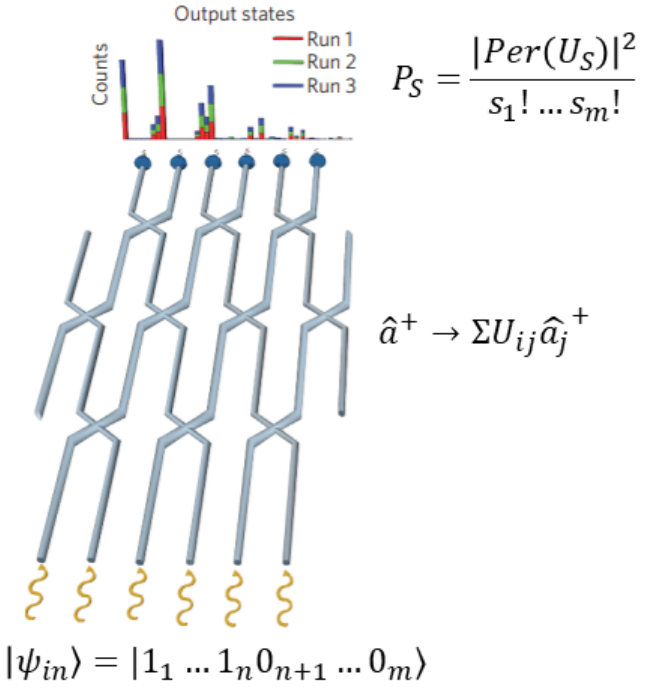

FIG. 1. Illustration of the boson-sampling problem. Adapted from [32].

that the probability of obtaining some configuration S is related to the matrix permanent of the transfer matrix that describes the relevant transformation, i.e.

$$P_S = |\alpha_S|^2 = \frac{|Per(U_S)|^2}{s_1! \dots s_m!} \tag{6}$$

where U_S is an $n \times n$ submatrix of U constructed by taking s_i copies of the ith column of U. This task is then repeated many times to sample from the output statistical distribution with a finite number of measurements.

B. Complexity of the Problem

Computing the exact matrix permanent is known to belong to the complexity class #P-hard, with the fastest reported algorithm running in $O(n^2 2^n)$ time for an $n \times n$ matrix [8], or $O(n2^n)$ if the matrix is processed in a certain order [9]. Thus, it is perhaps unsurprising that since the relevant probability distribution in boson-sampling depends on the square of a matrix permanent, a classical device cannot simulate the same task without exponential overhead. Specifically, AA showed that approximating the square of a matrix permanent to a multiplicative constant also belongs to the class #P-hard, and that if there existed a polynomial-time classical algorithm for exact boson-sampling, it would collapse the polynomial hierarchy [4]. As the polynomial hierarchy is founda-

tional to computational complexity theory, it is strongly believed that collapse is unlikely, thus providing strong evidence for the hardness of exact boson-sampling.

However, it is also well-established that the permanent of a matrix with real, non-negative entries can be efficiently estimated [4]. Considering that any real boson-sampling experiment would have errors and thus at best approximate the distribution, the question becomes: Can *approximate* classical simulation of the boson-sampling problem be achieved in polynomial time? It turns out that if the unitary transformation describing the interfometer is sufficiently "random", the answer is no. Briefly, consider a $m \times m$ Haar-random matrix. Then, $n \times n$ submatrices with $n \leq m^{1/6}$ are approximately Gaussian, i.e. the entries are close in variation distance to independent and identically distributed (iid) complex Gaussians $\mathcal{N}(0,1)_C$ [4]. As a result, the matrix does not have any special structure for a classical algorithm to exploit, and so it is conjectured that approximating the permanent of a Gaussian matrix is also #P-hard. Correspondingly, it is expected that the existence of an efficient classical algorithm for approximate boson-sampling would also collapse the polynomial hierarchy, and thus even approximate boson-sampling is classically intractable.

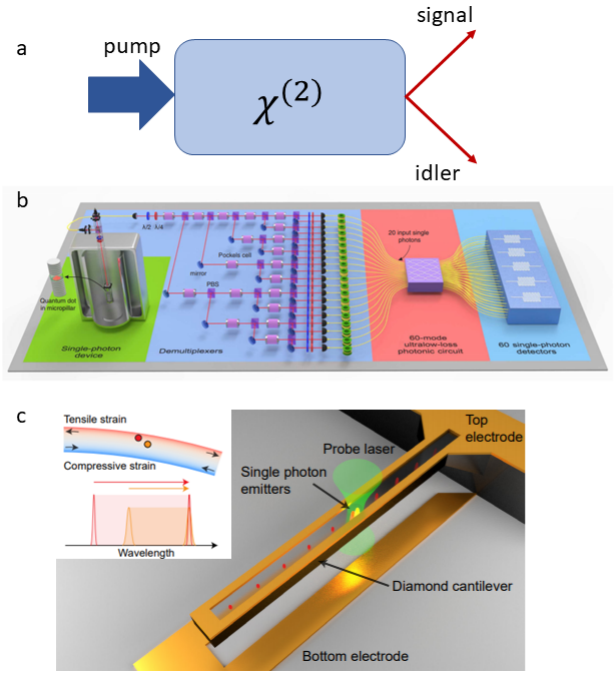

FIG. 2. Proposed single-photon sources. a) The mechanism of SPDC. b) Multiplexing of photon trains from quantum dots into different spatial modes, reproduced from [19] c) Strain can be used to reduce spectral inhomogeneity in an array of single-photon emitters, adapted from [20].

III. PHOTONIC IMPLEMENTATION OF EXPERIMENTAL BOSON-SAMPLING

Part of the appeal of boson-sampling lies in the relative simplicity of the required components. In general, all boson-sampling experiments can be split into three stages: 1) the preparation of the input Fock state, with each mode containing at most 1 photon, 2) the evolution of the state by a Haar-random unitary operator, and 3) the measurement of boson-number at all output modes. In the photonic implementation, the first stage requires reliable single-photon sources; the second, some form of a linear-optical network; and the third, high-efficiency photodetectors. In this section, we discuss progress and challenges facing these three components, as well as potential solutions.

A. Single-Photon Sources

Initial boson-sampling experiments primarily used spontaneous parametric downconversion (SPDC) as the chosen method for input state preparation. Briefly, in SPDC a second-order nonlinear crystal is used to convert photons from a pump beam into photons in two lower-energy modes, the signal and the idler (Fig. 2a). The output state is then

$$|\psi_{SPDC}\rangle = \sqrt{1-\chi^2}\sum_{n=0}^{\infty}\chi^n |n\rangle_s |n\rangle_i \qquad (7)$$

where χ is the squeezing parameter [10]. For single-photon generation, the desired term in the superposition is where $n = 1$, as the measurement of one photon can then be used to herald the arrival of the other single photon.

However, while well-established, SPDC suffers a number of drawbacks. In particular, the number of photons that can be generated is rather limited, with most experiments limited to three photons – with high enough pump powers, the nonlinear crystal can generate two simultaneous photon pairs in four different modes, with one photon used to herald the other three [11-15]. Higher numbers are unlikely, due to the probabilistic nature of the process: if single pair generation occurs with probability ϵ, then the simultaneous generation of n pairs occurs with exponentially decaying probability ϵ^n. Although this probability can be increased by simply increasing the pump intensity, this runs the risk of activating undesired higher-order nonlinear effects. As a result, solid-state single photon emitters have garnered increasing research interest in recent years. A comprehensive review can be found in reference [16]. These emitters typically arise in the form of quantum dots or defect centers in solids, thus combining the benefits of atom-like emission with scalable solid-state hosts. The key parameters of interest are the brightness, stability, indistinguishability, and single-photon purity. In particular, these emitters can be quite bright especially when embed-

ded in a cavity, i.e. they can generate photons at high rates. However, they come with their own challenges, particularly in the realms of indistinguishability and purity. Due to the complex many-body physics inherent to solid state hosts, there is inhomogeneity and thus photon distinguishability from different emitters. Moreover, with regards to purity, which dictates single vs multi-photon emission probabilities (higher purity corresponds to greater single-photon probability), only GaAs-based quantum dots have purities greater than 99% compared to values of 70-90% typical to other systems [16].

Still, numerous protocols have been developed recently that utilize such solid-state emitters, in particular arsenide-based quantum dots. It is worth nothing that this adds an additional constraint of IR-wavelength (900-1000 nm) operation, where such dots typically emit. State initilization can be achieved using mode-locked oscillators as the excitation, resulting in pulsed single-photon streams that are nearly identical. These photon trains can then be demultiplexed into different spatial modes using fast optical switches (Fig. 2b) [17-19]. This method was recently used to perform boson-sampling with 20 input photons, while maintaining purity and indistinguishability as high as 97.5% and 95.4%, respectively [19]. Alternatively, arrays of single-photon emitters can be excited simultaneously, similar to scatter-shot boson-sampling methods that utilize multiple SPDC sources. While spectral inhomogeneity is an issue, strain can be used to tune the emission of individual emitters, a technique which has already been demonstrated in diamond defect centers using nanoelectromechanical actuators (Fig. 2c) [20,21].

B. Linear-Optical Network

As a boson-sampling experiment large enough to demonstrate quantum supremacy would require hundreds of individual beamsplitters and phase-shifters, bulky discrete optical components are unlikely to be useful. Instead, experimental demonstrations of boson-sampling have overwhelmingly used integrated photonics (Fig. 3a) [12-15,22-23]. Haar-random unitaries can be mapped to beamsplitters and phaseshifters with classical computers. The vast majority of such devices then use fs or UV lasers to quickly micromachine the circuit into a substrate, using nonlinear absorption to change refractive indices locally [13]. Advances on the basic technique include three-dimensional waveguiding to achieve better independent control over each directional coupler [22], and fully reprogrammable photonic circuits composed of cascaded Mach-Zehnder interfometers controlled by thermo-optic phase shifters [23]. Such techniques enable the systems to apply any arbitrary m-mode unitary transformation.

These techniques inevitably suffer from in/out-coupling losses, as well as photon losses within the circuit. While not ideal, it is expected that simulating

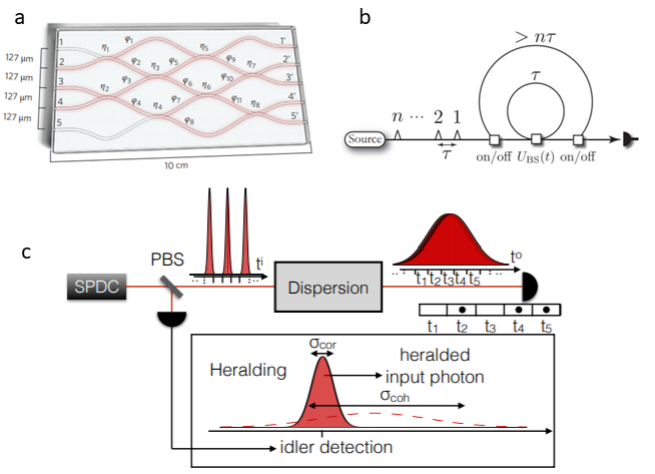

FIG. 3. Schemes for implementing the requisite Haar-random unitary transformation: a) Integrated photonics, reproduced from [12], b) Time-bin encoding, reproduced from [26], and c) Dispersive optics with heralded single photons, reproduced from [24].

boson-sampling even with losses is expected to be classically hard [13]. Moreover, low-loss optical circuitry has improved since the initial days of experimental boson-sampling, with a recent demonstration of 98.7% optical transmission using a 3D architecture composed of stacked fused quartz trapezoids [17-19]. Each interface contains a thin-film optical coating that effectively acts as a row of beamsplitters, achieving ultralow loss at the cost of reconfigurability and universality.

More exotic proposals also exist, although more work needs to be done before attaining widespread adoption (Fig. 3b, 3c). One proposal uses dispersive optics to perform boson sampling with temporal rather than spatial modes [24]. Specifically, the proposal draws an equivalence between boson-sampling and measuring the output time of heralded single photons passing through dispersive optics, which would greatly relax photon source and detector requirements. A different proposal uses time-bin encoding, where single photons arrive in a train of time bins [25,26]. A fiber loop with appropriate switching can then be used to introduce a time delay, moving photons between adjacent time bins and enabling them to interfere and vastly reducing the size of the experimental setup.

C. Photon Detectors

Photon detectors used in boson-sampling can generally be divided into two groups: on/off "bucket" detectors, and photon-number distinguishing detectors [27]. Photon-counting detectors are generally more expensive and difficult to make than bucket detectors. As a result, it is oft stated in the literature that for a n-photon

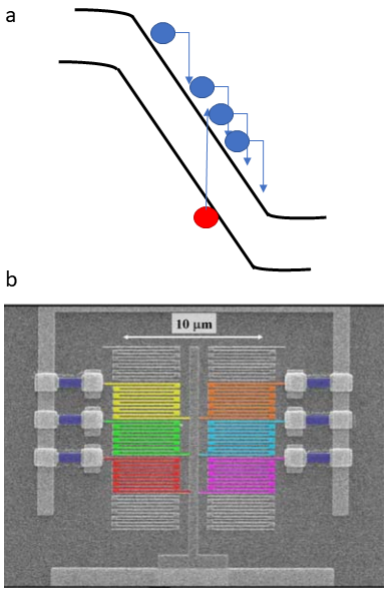

FIG. 4. Photon detection. a) Energy band diagram depicting impact ionization, the operating mechanism of SPADs. b) Parallel arrays of nanowires for photon-number discerning detectors. Reproduced from [29].

boson-sampling experiment, the number of modes should be $m >> n^2$. Under this condition, a straightforward counting argument suggests a "bosonic birthday paradox," where it becomes probabilistically unlikely for more than one boson to end up in the same final mode, and as such bucket detectors are sufficient [4]. However, this superquadratic growth in the number of modes precludes the scaling of boson-sampling experiments, and as such it may become relevant to resolve photon number. We thereby discuss both types of detectors in this section.

As a brief overview, the most common single-photon detectors used in boson-sampling are single-photon avalanche diodes (SPADs) and superconducting nanowire single-photon detectors (SNSPDs) [27]. SPADs operate by applying a large reverse-bias voltage to a photodiode, creating a steep potential gradient that enables a process known as impact ionization (Fig. 4a). Essentially, the device operates in a analogous manner to a photomultiplier tube: photoexcited carriers accelerate due to the gradient, scatter off the lattice and ionize more carriers, thereby inducing a large current spike. SNSPDs operate on the principle of superconductivity: a nanowire of superconducting material is cooled to just below its critical temperature T_c. If a photon is absorbed, the added energy raises the temperature locally above T_c and changes the resistance in a detectable manner. Both implementations can be used as bucket detectors. In fact, even if only bucket detectors are available, the issue of photon number resolution can be addressed using postselection [4]. That is, if n photons are known to have been injected, filter out outputs where the number of bucket detections are not exactly n. This of course depends greatly on the detection efficiency, with the need for postselection decreasing as the efficiency approaches unity. In this realm SNSPDs offer a clear advantage, with reported IR wavelength detection efficiencies $> 93\%$ [28], whereas silicon SPADs offer a peak efficiency of 65% at 650 nm [27]. But since detector efficiency remains an active area of research, it is conceivable that semiconductor-based SPADs will improve their efficiencies to approach that of SNSPDs, mitigating the high cost and complexity of the latter.

In terms of number-resolving detectors, SNSPDs are typically used. Since the resistance will change proportionally to the number of photons absorbed, superconductivity inherently offers a natural way of photon counting [27]. The issue is that if the entire nanowire temperature increases above T_c, all superconductivity is lost and the photon number saturates. This can potentially be mitigated by using parallel arrays of nanowires, each connected in series to a resistor (Fig. 4b) [29,30].

IV. APPLICATIONS

It is telling that in one of the early papers on boson-sampling, the authors concluded their abstract with the curt phrase that boson-sampling "could lead to applications" [10]. Beyond demonstrating quantum supremacy, the practical usefulness of boson-sampling seemed dubious. In this section, we discuss recent experimental progress in boson-sampling toward quantum supremacy, as well as recent work outside boson-sampling's original context. We conclude that the boson-sampling platform shows great promise for applications in diverse fields such as simulation and cryptography.

A. Quantum Supremacy

In Table 1 we summarize recent progress in experimental boson-sampling. We note that the number of input photons n and modes m has increased monotonically with time, most recently reaching a peak of $n = 20$, $m = 60$ with 14 photons routinely detected at the output. Corresponding to a Hilbert space of size 3.7×10^{14} (48 qubits), this experiment was the first boson-sampling experiment such that all output combinations could not be exhausted [19]. Note that the threshold number of photons for unequivocal quantum supremacy is expected to be around $n = 50$ [31].

This result came just after Google's claim of quantum supremacy in 2019. Using a 53-qubit superconducting processor, they performed the task of sampling from the output distribution of random circuits, which is also expected to be classically hard to simulate [5]. Although this claim is hotly debated, it certainly detracts from boson-sampling's original purpose: to be the fastest route toward demonstrating unambiguous quantum advantage.

TABLE I. Experimental progress toward quantum supremacy using boson-sampling. Note that n refers to the number of *detected* photons, while m refers to the number of modes.

Work	Year	n	m
Tillman et al. [12]	2013	3	5
Crespi et al. [13]	2013	3	5
Broome et al. [14]	2013	3	6
Spring et al. [15]	2013	3	6
Carolan et al. [22]	2014	3	9
Carolan et al. [23]	2015	3	6
Wang et al. [17]	2017	5	9
Wang et al. [18]	2018	5	16
Wang et al. [19]	2019	14	60

Google's results thus provide timely motivation to discover new applications for boson-sampling.

B. Molecular Simulation

Boson-sampling has particularly apt application as a method of simulating molecular vibronic spectra [32-35]. In particular, as mentioned before the boson-sampling problem is not relegated to the optical domain – in other words, n photons in m optical modes is isomorphic to n phonons in m vibrational modes. However, while boson-sampling amounts to a rotation of the mode operators $\hat{a}^{\dagger\prime} = U\hat{a}^\dagger = \hat{R}_U^\dagger \hat{a}^\dagger \hat{R}_U$, because an electronic transition in a molecule causes nuclear structural changes, the transformation is more complicated. Specifically, the mode can be displaced, distorted (squeezed), and rotated. Huh et al. showed that this can be accounted for by simply altering the input state to be a squeezed coherent state

$$\begin{aligned} |\psi_{in}\rangle &= \hat{S}_\Sigma^\dagger \hat{R}_{C_R}^\dagger \hat{D}_{J^{-1}\delta/\sqrt{2}} |0\rangle \\ &= \hat{S}_\Sigma^\dagger |\frac{1}{\sqrt{2}} C_R^\dagger J^{-1}\delta\rangle \end{aligned} \tag{8}$$

where $\hat{S}_\Sigma^\dagger$, $\hat{R}_{C_R}^\dagger$, and $\hat{D}_{J^{-1}\delta/\sqrt{2}}$ are squeezing, rotation, and displacement operators parametrized by the specific molecular system being discussed [32]. The boson-sampling linear optical network then serves as a final rotation to bring the system to the desired state before measurement. An example for formic acid is shown in Figure 5a.

This technique was recently used by Paesani et al. to benchmark the quality of squeezed light produced on a silicon chip [35]. Due to the low level of squeezing achievable, most of the contributions came from vacuum, which is a classically tractable problem. Thus, the improvement in fidelity over a classical simulation method was minimal. More experimental work should be done toward improving the quality of squeezing in order for boson-sampling to show a clear speedup in the task of simulating vibronic spectra.

Moreover, the initial insight that boson-sampling can use any boson, not just photons, is quite general. We envision that photonic boson-sampling can potentially be used to study many other bosonic systems. In particular, the original boson-sampling proposal has inspired numerous alternative experiments that solve an equivalent problem with a different physical system, such as interacting spins [36]. The success of one system could lead to insights into the others.

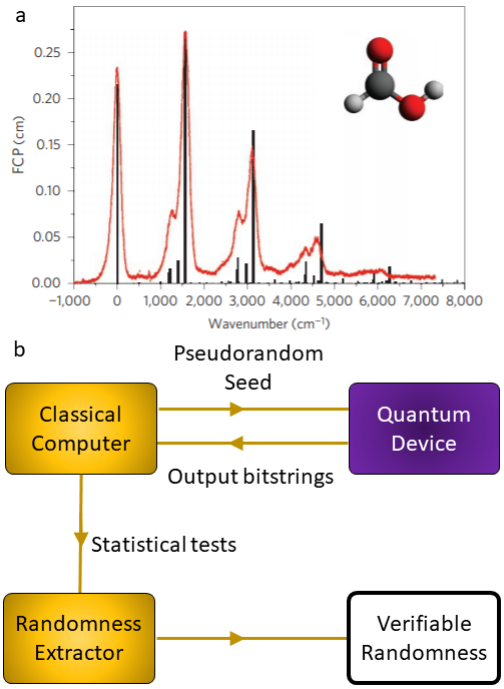

FIG. 5. Boson-sampling beyond quantum supremacy. a) The mechanism of boson-sampling has a deep connection to molecular vibronic spectra. A comparison of the results of boson-sampling vs. measured formic acid spectra are shown. Reproduced from [32]. b) Proposal for generating verifiable randomness from quantum supremacy demonstrations using sampling problems. A pseudorandom seed from a classical computer can be used to generate random circuits or beam-splitter networks. A quantum device performs a task such as random circuit sampling or boson-sampling and sends the output to a classical computer. The classical computer verifies the randomness and uses the high-entropy output to seed a randomness extractor.

C. Cryptography

Boson-sampling has no known applications in cryptography. Specifically, boson-sampling is typically viewed from the perspective of a sampling problem, whereas modern cryptography is based on function problems, such as prime factorization, and the related concept of decision problems. Roughly, decision problems are problems where the answer is a binary "yes/no" for each input. As an example, RSA encryption is predicated on the assumption that there is no efficient classical algorithm

for factoring large numbers [37]. Therefore, it remains an open question to discover a decision problem that boson-sampling can solve efficiently while a classical computer cannot.

However, recent theoretical work has shown that this path has promise, with Nikolopoulos & Broughham defining a general theoretical framework for for the design of boson-sampling based decision/function problems [38]. Briefly, their framework involves dividing all possible output configurations into separate bins, and asking questions about the most probable bin. As estimating the most probable bin likely requires brute-force calculation of output probabilities and thus matrix permanents, it is expected (although not rigorously proved!) that problems in this framework will be classically intractable.

Finally, it was recently suggested that quantum supremacy can be used to generate verifiable random numbers [39-40]. This would find particular application in both classical and quantum cryptography, as well as scientific applications such as reliable Monte Carlo simulations and commercial applications such as gambling [41]. Specifically, Aaronson and Chen recently showed that the outputs of random circuit sampling pass a statistical test, Heavy Output Generation (HOG), that no efficient classical algorithm can [39]. In essence, the test indicates that no classical computer can generate the same amount of entropy that random circuit sampling does in a comparable time, thereby providing a method of "verifying" randomness. The outline of the proposal is then as follows: 1) Use a trusted classical computer to pseudorandomly generate quantum circuits, 2) perform random circuit sampling on those circuits, 3) check for high entropy in the output bitstrings using HOG, and 4) if the statistical tests pass, use the output bitstrings to seed a classical randomness extractor [40].

One can easily draw a parallel between random circuit sampling and boson sampling, and surmise that boson sampling could play a similar role in generating verifiable randomness (Fig. 5b). To date though, there is no similar statistical test to HOG for boson-sampling that refers to the measured outputs of the task, as opposed to the distribution being sampled [38]. If such a test were to be developed, we envision that boson-sampling will provide an appealing alternative for verifiable random number generation, for the same reasons that it is a strong candidate for quantum supremacy: namely, the relative simplicity of the implementation and the speed of operation.

V. CONCLUSION

In conclusion, we have provided an overview of boson-sampling. We discuss progress, challenges, and potential solutions in the photonic implementation of experimental boson-sampling. Over the years, the complexity of boson-sampling experiments have grown rapidly, and we expect that with further improvements to the requisite single-photon sources, integrated optics, and detectors, the sample space will only continue to grow. On the application side, much theoretical work needs to be done to expand boson-sampling to domains such as molecular simulation, cryptography, and random-number generation. Still, we conclude that boson-sampling has great potential for applications beyond quantum supremacy.

[1] M. A. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2002).
[2] D. P. DiVincenzo, Fortschritte der Physik: Progress of Physics **48**, 771 (2000).
[3] E. Knill, R. Laflamme and G. J. Milburn, Nature **409**, 46 (2001).
[4] S. Aaronson and A. Arkhipov, in *Proceedings of the ACM Symposium on Theory of Computing* (ACM, New York, 2011) p. 333342.
[5] F. Arute, et al., Nature **574(7779)**, 505 (2019).
[6] C. G. Gerry and P. L. Knight, *Introductory Quantum Optics* (Cambridge University Press, 2005).
[7] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, Phys. Rev. Lett. **73(1)**, 58 (1994).
[8] H. J. Ryser, in *Combinatorial Mathematics*, Vol. 14 (American Mathematical Soc., 1963).
[9] A. Björklund, in *Proceedings of the twenty-third annual ACM-SIAM symposium on Discrete Algorithms*, Vol. 14 (Society for Industrial and Applied Mathematics, 2012).
[10] A. P. Lund, et al., Phys. Rev. Lett. **113(10)**, 100502 (2014).
[11] D. J. Brod, et al., Adv. Phot. **1(3)**, 034001 (2019).
[12] M. Tillman, et al., Nat. Phot. **7(7)**, 540 (2013).
[13] A. Crespi, et al., Nat. Phot. **7(7)**, 545 (2013).
[14] M. A. Broome, et al., Science **339(6121)**, 794 (2013).
[15] J. B. Spring, et al., Science **339(6121)**, 798 (2013).
[16] I. Aharonovich, D. Englund and M. Toth, Nat. Phot. **10(10)**, 631 (2016).
[17] H. Wang, et al., Nat. Phot. **11**, 361 (2017).
[18] H. Wang, et al., Phys. Rev. Lett. **120(23)**, 230502 (2018).
[19] H. Wang, et al., Phys. Rev. Lett. **123(25)**, 250503 (2019).
[20] S. Maity, et al., Phys. Rev. Appl. **10(2)**, 024050 (2018).
[21] N. H. Wan, et al., arXiv preprint arXiv:1911.05265 (2019).
[22] J. Carolan, et al., Nat. Phot. **8**, 621 (2014).
[23] J. Carolan, et al., Science **349(6249)**, 711 (2015).
[24] M. Pant and D. Englund, Phys. Rev. A **93(4)**, 043803 (2016).
[25] Y. He, et al., Phys. Rev. Lett. **118**, 190501 (2017).
[26] K. R. Motes, et al., Phys. Rev. Lett. **113(12)**, 120510 (2014).
[27] R. H. Hadfield, Nat. Phot. **3(12)**, 696 (2009).
[28] F. Marsili, et al., Nat. Phot. **7(3)**, 210 (2013).

[29] A. Divochiy, et al., Nat. Phot. **2(5)**, 302 (2008).
[30] D. Zhu, et al., Nano Lett. **10(1021)**, 0c00985 (2020).
[31] A. Neville, et al., Nat. Phys. **13(12)**, 1153 (2017).
[32] J. Huh, et al., Nat. Phys. **9(9)**, 615 (2015).
[33] J. Huh and M.-H. Yung, Sci. Rep. **7(1)**, 1 (2017).
[34] C. S. Hamilton, et al., Phys. Phys. Lett. **119(17)**, 170501 (2017).
[35] S. Paesani, et al., Nat. Phys. **15(9)**, 925 (2019).
[36] B. Peropadre, A. Aspuru-Guzik, and J. J. Garcia-Ripoll, Phys. Rev. A **95(3)**, 032327 (2017).
[37] R. L. Rivest, A. Shamir, and L. Adleman, Communications of the ACM **21(2)**, 120 (1978).
[38] G. M. Nikolopoulos and T. Brougham, Phys. Rev. A **94(1)**, 012315 (2016).
[39] S. Aaronson and L. Chen, arXiv preprint arXiv:1612.05903 (2016).
[40] S. Aaronson, Aspects of certified randomness from quantum supremacy (2019), see https://www.scottaaronson.com/talks/.
[41] M. Herrero-Collantes and J. C. Garcia-Escartin, Rev. Mod. Phys. **89(1)**, 015004 (2017).