matrices for this graph at momenta $-\pi/4$ and $-\pi/2$ are

$$S_{\text{switch}}(-\pi/4) = \begin{pmatrix} 0 & 0 & e^{-i\pi/4} \\ 0 & -1 & 0 \\ e^{-i\pi/4} & 0 & 0 \end{pmatrix}$$

$$S_{\text{switch}}(-\pi/2) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix} \quad (5)$$

The momentum switch has perfect transmission between vertices 1 and 3 at momentum $-\pi/4$ and perfect transmission between vertices 2 and 3 at momentum $-\pi/2$. Thus, the path a particle follows through the switch depends on its momentum: A particle with momentum $-\pi/2$ follows the double line in Fig. 3A, whereas a particle with momentum $-\pi/4$ follows the single line.

The graph used to implement the Cθ gate is shown in Fig. 3B [see section S4 of (*32*) for the numbers of vertices on each of the paths]. To see why this graph implements a Cθ gate, consider the movement of two particles as they pass through the graph. If either particle begins in the state $|0_{\text{in}}\rangle$, it travels along a path to the output without interacting with the second particle. When either particle begins in the state $|1_{\text{in}}\rangle$, it is routed onto the vertical path as it passes through the first momentum switch and is routed to the right as it passes through the second switch. If both particles begin in the state $|1_{\text{in}}\rangle$, they interact on the vertical path and the wave function acquires a phase $e^{i\theta}$.

To implement a circuit, the subgraphs representing circuit elements are connected by paths. Figure 4 depicts a graph corresponding to a simple two-qubit computation. Timing is important: Wave packets must meet on the vertical paths for interactions to occur. We achieve this by choosing the numbers of vertices on each of the segments in the graph appropriately, taking into account the different propagation speeds of the two wave packets [see section S4 of (*32*)]. In section S3.1 of (*32*), we present a refinement of our scheme using planar graphs with maximum degree four.

By analyzing the full $(n + 1)$–particle interacting many-body system, we prove that our algorithm performs the desired quantum computation up to an error term that can be made arbitrarily small (*32*). Our analysis goes beyond the scattering theory discussion presented above; we take into account the fact that both the wave packets and the graphs are finite. Specifically, we prove that by choosing the size of the wave packets, the number of vertices in the graph, and the total evolution time to be polynomial functions of both n and g, the error in simulating an n-qubit, g-gate quantum circuit is bounded above by an arbitrarily small constant [section S5 of (*32*)]. For example, for the Bose-Hubbard model and for the nearest-neighbor interaction model, we prove that the error can be made arbitrarily small by choosing the size of the wave packets to be $O(n^{12}g^4)$, the total number of vertices in the graph to be $O(n^{13}g^5)$, and the total evolution time to be $O(n^{12}g^5)$. The bounds we prove, although almost certainly not optimal, are sufficient to establish universality with only polynomial overhead. Because it is also possible to efficiently simulate a multiparticle quantum walk of the type we consider using a universal quantum computer, this model exactly captures the power of quantum computation.

References and Notes

1. E. Farhi, S. Gutmann, *Phys. Rev. A* **58**, 915 (1998).
2. D. Aharonov, A. Ambainis, J. Kempe, U. Vazirani, "Quantum walks on graphs," *Proceedings of the 33rd ACM Symposium on Theory of Computing* (2001), pp. 50–59.
3. A. Ambainis, E. Bach, A. Nayak, A. Vishwanath, J. Watrous, "One-dimensional quantum walks," *Proceedings of the 33rd ACM Symposium on Theory of Computing* (2001), pp. 37–49.
4. A. M. Childs *et al.*, "Exponential algorithmic speedup by quantum walk," *Proceedings of the 35th ACM Symposium on Theory of Computing* (2003), pp. 59–68.
5. A. Ambainis, *SIAM J. Comput.* **37**, 210 (2007).
6. E. Farhi, J. Goldstone, S. Gutmann, *Theory of Computing* **4**, 169 (2008).
7. A. M. Childs, *Phys. Rev. Lett.* **102**, 180501 (2009).
8. B. Do *et al.*, *J. Opt. Soc. Am. B* **22**, 499 (2005).
9. M. Karski *et al.*, *Science* **325**, 174 (2009).
10. H. B. Perets *et al.*, *Phys. Rev. Lett.* **100**, 170506 (2008).
11. Y. Bromberg, Y. Lahini, R. Morandotti, Y. Silberberg, *Phys. Rev. Lett.* **102**, 253904 (2009).
12. A. Peruzzo *et al.*, *Science* **329**, 1500 (2010).
13. J. O. Owens *et al.*, *New J. Phys.* **13**, 075003 (2011).
14. L. Sansoni *et al.*, *Phys. Rev. Lett.* **108**, 010502 (2012).
15. I. L. Chuang, Y. Yamamoto, *Phys. Rev. A* **52**, 3489 (1995).
16. G. K. Brennen, C. M. Caves, P. S. Jessen, I. H. Deutsch, *Phys. Rev. Lett.* **82**, 1060 (1999).
17. W. S. Bakr, J. I. Gillen, A. Peng, S. Fölling, M. Greiner, *Nature* **462**, 74 (2009).
18. A. J. Hoffman *et al.*, *Phys. Rev. Lett.* **107**, 053602 (2011).
19. J. K. Gamble, M. Friesen, D. Zhou, R. Joynt, S. N. Coppersmith, *Phys. Rev. A* **81**, 052313 (2010).
20. J. Smith, *Electron. Notes Discrete Math.* **38**, 795 (2011).
21. Y. Omar, N. Paunković, *Phys. Rev. A* **74**, 042304 (2006).
22. P. K. Pathak, G. S. Agarwal, *Phys. Rev. A* **75**, 032351 (2007).
23. Y. Lahini *et al.*, *Phys. Rev. A* **86**, 011603 (2012).
24. A. Schreiber *et al.*, *Science* **336**, 55 (2012).
25. A. Ahlbrecht *et al.*, *New J. Phys.* **14**, 073050 (2012).
26. P. P. Rohde, A. Schreiber, M. Štefaňák, I. Jex, C. Silberhorn, *New J. Phys.* **13**, 013001 (2011).
27. B. M. Terhal, D. P. DiVincenzo, *Phys. Rev. A* **65**, 032325 (2002).
28. S. Aaronson, A. Arkhipov, "The computational complexity of linear optics," *Proceedings of the 43rd ACM Symposium on Theory of Computing* (2011), pp. 333–342.
29. R. Ionicioiu, P. Zanardi, *Phys. Rev. A* **66**, 050301 (2002).
30. A. Mizel, D. A. Lidar, M. Mitchell, *Phys. Rev. Lett.* **99**, 070502 (2007).
31. A. M. Childs, D Gosset, *J. Math. Phys.* **53**, 102207 (2012).
32. Materials and methods are available as supplementary materials on *Science* Online.
33. M. Valiente, *Phys. Rev. A* **81**, 042102 (2010).
34. B. A. Blumer, M. S. Underwood, D. L. Feder, *Phys. Rev. A* **84**, 062302 (2011).

Acknowledgments: This work was supported in part by MITACS; Natural Sciences and Engineering Research Council of Canada; the Ontario Ministry of Research and Innovation; the Ontario Ministry of Training, Colleges, and Universities; and the U.S. Army Research Office.

Supplementary Materials

www.sciencemag.org/cgi/content/full/339/6121/791/DC1
Materials and Methods
Supplementary Text
Figs. S1 to S10
References

10 September 2012; accepted 17 December 2012
10.1126/science.1229957

Photonic Boson Sampling in a Tunable Circuit

Matthew A. Broome,[1,2]* Alessandro Fedrizzi,[1,2] Saleh Rahimi-Keshari,[2] Justin Dove,[3] Scott Aaronson,[3] Timothy C. Ralph,[2] Andrew G. White[1,2]

Quantum computers are unnecessary for exponentially efficient computation or simulation if the Extended Church-Turing thesis is correct. The thesis would be strongly contradicted by physical devices that efficiently perform tasks believed to be intractable for classical computers. Such a task is boson sampling: sampling the output distributions of *n* bosons scattered by some passive, linear unitary process. We tested the central premise of boson sampling, experimentally verifying that three-photon scattering amplitudes are given by the permanents of submatrices generated from a unitary describing a six-mode integrated optical circuit. We find the protocol to be robust, working even with the unavoidable effects of photon loss, non-ideal sources, and imperfect detection. Scaling this to large numbers of photons should be a much simpler task than building a universal quantum computer.

A major motivation for scalable quantum computing is Shor's algorithm (*1*), which enables the efficient factoring of large composite numbers into their constituent primes. The presumed difficulty of this task is the basis of the majority of today's public-key encryption schemes. It may be that scalable quantum computers are not realistic if, for example, quantum mechanics breaks down for large numbers of qubits (*2*). If, however, quantum computers are realistic physical devices, then the Extended Church-Turing (ECT) thesis—that any function efficiently computed on a realistic physical device can be efficiently computed on a probabilistic Turing machine—means that a classical efficient factoring algorithm exists. Such an algorithm, long sought after, would enable us to break public-key cryptosystems such as RSA. A third possibility is that the ECT thesis itself is wrong.

How do we answer this trilemma? As yet there is no evidence that large-scale quantum computers are inherently impossible (that will need to be tested directly via experiment), and there is no efficient classical factoring algorithm or mathematical proof of its impossibility. This leaves examining the validity of the ECT thesis, which would be contradicted, for example, by building a physical device that efficiently performs a task thought to be intractable for classical computers.

One such task is boson sampling: sampling from the probability distribution of n identical bosons scattered by some linear unitary process, U. The probabilities are defined in terms of permanents of $n \times n$ submatrices of U [in general, calculating these is exponentially difficult, because calculating the permanent is a so-called "#P-complete" problem (*3*); a class above even "NP-complete" in complexity] and is therefore strongly believed to be intractable. This does not mean that boson sampling is itself #P-complete: The ability to sample from a distribution need not imply the ability to calculate the permanents that gave rise to it. However, by using the fact that the permanent is #P-complete, (*4*) recently showed that the existence of a fast classical algorithm for this "easier" sampling task leads to drastic consequences in classical computational complexity theory, notably collapse of the polynomial hierarchy.

We tested the central premise of boson sampling, experimentally verifying that the amplitudes of $n = 2$ and $n = 3$ photon scattering events are given by the permanents of $n \times n$ submatrices of the operator U describing the physical device. We find the protocol to be robust, working even with imperfect sources, optics, and detectors.

Consider a race between two participants: Alice, who only possesses classical resources, and Bob, who in addition possesses quantum resources. They are given some physical operation, described by an evolution operator, U, and agree on a specific n-boson input configuration. Alice calculates an output sample distribution with a classical computer; Bob either builds or programs an existing linear photonic network, sending n single photons through it and obtaining his sample by measuring the output distribution (Fig. 1A). The race ends when both return samples from the distribution: The winner is whoever returns a sample fastest. As n becomes large, it is conjectured that Bob will always win, because Alice's computation runtime increases exponentially, whereas Bob's experimental runtime does not. It becomes intractable to verify Bob's output against Alice's, and, unlike for Shor's algorithm, there is no known efficient algorithm to verify the result (*4*). However, one can take a large instance—large enough for verification via a classical computer—and show that Bob's quantum computer solves the problem much faster, thereby strongly suggesting that the same behavior will continue for larger systems, casting serious doubt on the ECT thesis. In a fair race, Bob must verify that his device actually implements the target unitary; an alternative fair version is to give both Alice and Bob the same physical device instead of a mathematical description and have Alice characterize it before she predicts output samples via classical computation. Alice can use a characterization method that neither requires nonclassical resources nor adds to the complexity of the task (*5*).

We tested boson sampling using an optical network with $m = 6$ input and output modes and $n = 2$ and $n = 3$ photon inputs. We implemented a randomly chosen operator so that the permanents could not be efficiently calculated (*6*); that is, the elements are complex-valued and the operator U is fully connected, with every input distributed to every output. The 6-input × 6-output modes of U are represented by two orthogonal polarizations in 3 × 3 spatial modes of a fused-fiber beamsplitter (FBS), an intrinsically stable and low-loss device. The mode mapping is $\{1,...,6\} = \{|H\rangle_1,|V\rangle_1,|H\rangle_2,|V\rangle_2,|H\rangle_3,|V\rangle_3\}$, where $|H\rangle_1$ is the horizontally polarized mode for spatial mode 1. We can use polarization controllers at the inputs and outputs of the central 3 × 3 FBS to modify the evolution (see the equivalent circuit diagram in Fig. 1B).

Alice calculates the probability of bosonic scattering events in the following way (*4, 7*). Having characterized the evolution U using the method detailed in supplementary materials section S1 (*8*), and given the input and output configurations $S = (s_1,...,s_m)$ and $T = (t_1,...,t_m)$ with boson occupation numbers s_i and t_j respectively, she produces an $n \times m$ submatrix U_T by taking t_j copies of the j^{th} column of U. Then, she forms the $n \times n$ submatrix U_{ST} by taking s_i copies of the i^{th} row of U_T. The probability for the scattering event T, for indistinguishable input photons S, is given by $P_T^Q = |\mathrm{Per}(U_{ST}|^2$. Conversely, the classical scattering probabilities when the input photons are distinguishable are given by $P_T^C = \mathrm{Per}(\tilde{U}_{ST})$, where $\tilde{U}_{ST_{ij}} = |U_{ST_{ij}}|^2$.

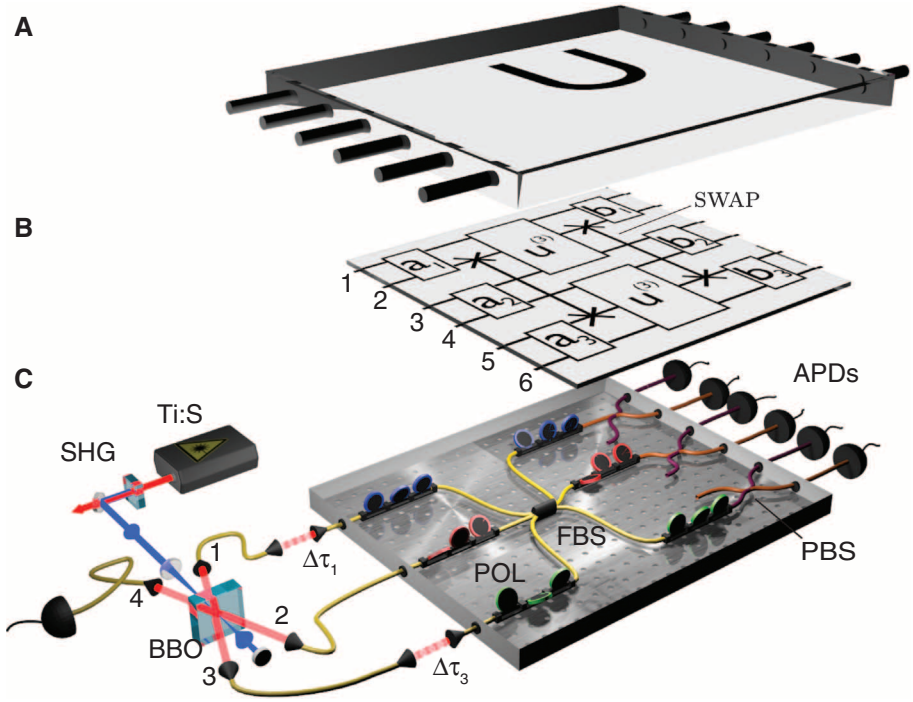

Fig. 1. Experimental scheme for boson sampling. (**A**) Both Alice and Bob (possessing classical and quantum resources, respectively) must sample the output distribution from some unitary, U. (**B**) Equivalent circuit. The orthogonal polarizations in each input spatial mode can be arbitrarily combined by the unitaries $a_1 \ldots a_3$. A multiport, $u^{(3)}$, interferes all modes of the same polarization; orthogonal polarizations are recombined by $b_1 \ldots b_3$. (**C**) Experiment. Photons are produced via downconversion in a nonlinear crystal (BBO) pumped by a frequency-doubled (SHG) laser (Ti:S) (*8*). Photon 4 acts as a trigger and photons 1 to 3 are inputs; 1 and 3 can be delayed or advanced with respect to photon 2 by $\Delta\tau_1$, $\Delta\tau_3$, respectively. Local unitaries $a_1 \ldots b_3$ are implemented with polarization controllers (POL); $u^{(3)}$ is implemented by a 3 × 3 nonpolarizing FBS; three polarizing fiber beam-splitters (PBS) output six spatial modes to single-photon avalanche diodes (APDs). The fiber beam-splitters work by evanescent coupling between multiple input fibers in close proximity.

[1]Centre for Engineered Quantum Systems, School of Mathematics and Physics, University of Queensland, Brisbane, Queensland 4072, Australia. [2]Centre for Quantum Computation and Communication Technology, School of Mathematics and Physics, University of Queensland, Brisbane, Queensland 4072, Australia. [3]Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology, Cambridge, MA 02139, USA.

*To whom correspondence should be addressed. E-mail: m.a.broome@googlemail.com

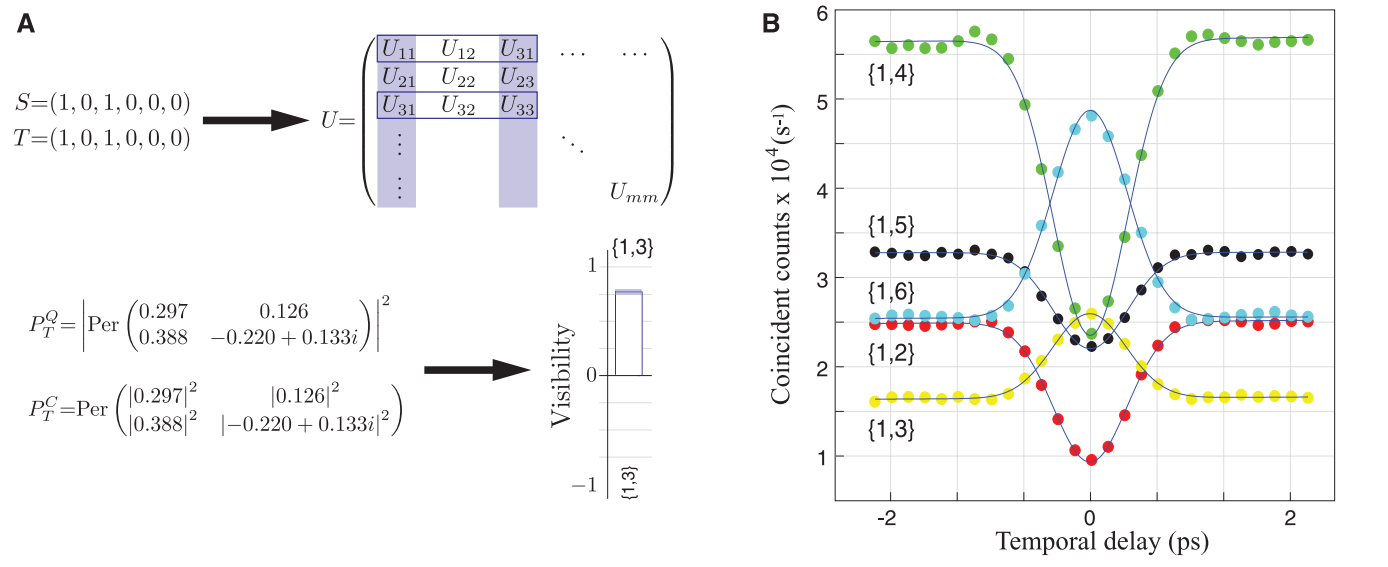

Fig. 2. Two-photon boson sampling. (**A**) Outline of Alice's technique to predict visibilities from the unitary evolution *U* (*8*). For photons input and output in modes 1 and 3, her prediction is given by the bar at bottom right; its uncertainty, obtained by 10 separate characterizations of the unitary, is represented by the shaded box on top of the bar. (**B**) Two-photon quantum interferences: the five output combinations {1,*m*} for the input configuration of {1,5}. Errors are smaller than marker size, and the solid blue lines are Gaussian fits used to calculate the visibility from Eq. 1. (**C**) Alice's predictions (blue line envelope) and Bob's measurements (orange bars) of two-photon visibilities. Input configurations are shown at the top left of each panel; output modes are labeled at the plot bottom. Errors are given by light blue and dark red boxes at the extremes of each data set. Yellow circles are the visibility predictions, given coherent input states.

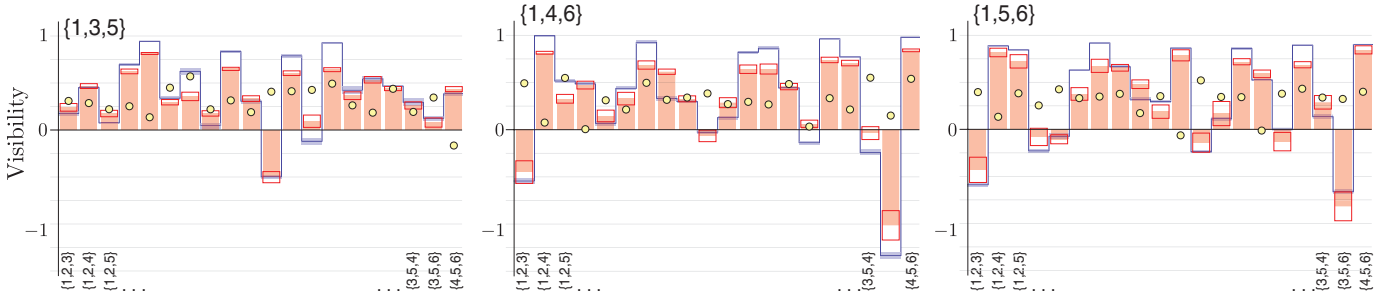

Fig. 3. Three-photon boson sampling. Alice's predictions (blue line envelope) and Bob's measurements (orange bars) for three-photon visibilities are shown. Labels, errors, and symbols are as defined in Fig. 2C).

Bob, on the other hand, experimentally prepares the *n*-photon Fock state $|t_1,\ldots,t_m\rangle$. After injecting the desired input to the circuit, he determines the probability of the scattering event *T* by projecting onto its corresponding state using single-photon detectors connected to a coincidence-counting logic. We prepared near–single-photon Fock states via spontaneous parametric downconversion in a nonlinear crystal [Fig. 1C, and for further details, see section S2 (*8*)]. Once the photons pass through the network, they are detected by single-photon avalanche diodes. The boson sampling protocol measures the frequency of output events; i.e., raw coincident photon counts. These, however, are strongly affected by differences in efficiency between photon counters, an effect that can be removed by measuring nonclassical interference visibility instead

$$V_T = \frac{P_T^C - P_T^Q}{P_T^C} \quad (1)$$

where P_T^Q and P_T^C are the quantum and classical probabilities for the output configuration *T* measured for completely indistinguishable and distinguishable photons, respectively. Distinguishable statistics are obtained by introducing a temporal delay, $\Delta\tau$, between the input photons. When all photons are delayed by significantly more than their respective coherence lengths, *L*, true two-photon quantum interference cannot occur. Figure 2A outlines the technique Alice uses to predict the visibility from the unitary evolution *U*. For $n = 2$, high count rates mean that 27 samples of the output *T* were taken as the temporal delay was changed between the two input photons

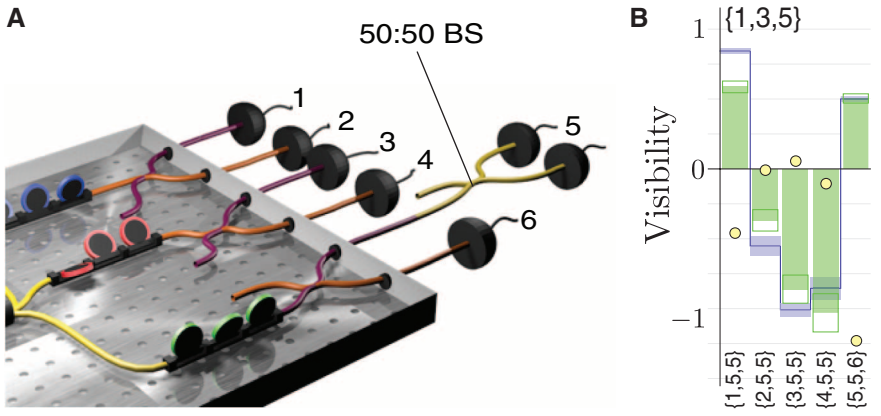

Fig. 4. Three-photon boson sampling with colliding outputs. (**A**) Number resolution was achieved with a 50:50 FBS in mode 5 and an additional detector. An imperfect splitting ratio for this FBS impedes only the effective efficiency of our number-resolving scheme (*10*, *11*). (**B**) For an input configuration {1,3,5}, and measuring two photons in output 5, the solid blue-line envelope shows Alice's predictions; the green bars are Bob's measured visibilities. Labels, errors, and symbols are as defined in Fig. 2C.

(*9*). For $n = 3$, where we used three of the photons from a four-photon state, low count rates mean that only three measurements were taken to avoid optical misalignment and the signal drift that occurs over necessarily long experimental runtimes. Therefore, for $n = 2$, the visibilities are calculated from the fitted Gaussian curves (Fig. 2B); for $n = 3$, the probabilities P_T^C are obtained from just two measurement settings: (i) $P_T^C = \{-\Delta\tau_\infty,0,\Delta\tau_\infty\}$ and (ii) $P_T^C = \{\Delta\tau_\infty,0,-\Delta\tau_\infty\}$, where $\{\tau_1,\tau_2,\tau_3\}$ are the temporal delays of photons 1, 2, and 3 with respect to photon 2, and $\Delta\tau_\infty >> L/c$. P_T^C is calculated as the average of these two probabilities to account for optical misalignment. Accordingly, P_T^Q is obtained with a single measurement of the output frequencies for completely indistinguishable photons, given by the delays $\{0,0,0\}$.

Figure 2C shows Alice's predictions and Bob's measurements for $n = 2$. We compare their results using the average L_1-norm distance per output configuration, $\mathcal{L}_1 = \frac{1}{C(m,n)}\sum_T |V_T^A - V_T^B|$, where $C(m,n)$ is the binomial coefficient [section S3 (*8*)]. We find excellent agreement between Alice and Bob, with the average across these three configurations being $\overline{\mathcal{L}}_1 = 0.021 \pm 0.001$. Next we show that if Alice uses her classically powerful resources, such as coherent states from a laser [section S4 (*8*)], to perform an analogous experiment to Bob's, she will not obtain the same results. Her classical predictions, given by the yellow circles in Fig. 2C, are markedly different from Bob's quantum measurements, with $\overline{\mathcal{L}}_1 = 0.548 \pm 0.006$. This large, statistically significant disagreement highlights the fact that Bob is accurately sampling from a highly nonclassical distribution.

Figure 3 shows the results for $n = 3$: There is a larger average distance between Alice and Bob's distributions, $\overline{\mathcal{L}}_1 = 0.122 \pm 0.025$, and consequently a smaller distance between Alice's classical predictions and Bob's measurements, $\overline{\mathcal{L}}_1 = 0.358 \pm 0.086$. We attribute these changes chiefly to the increased ratio of higher-order photon emissions in the three-photon input as compared with the two-photon case [section S5 (*8*)]. Having tested all possible noncolliding output configurations (that is, one photon per output-mode), we also tested colliding configurations, with two photons per output-mode. This requires photon-number resolution (*10*, *11*), using the method shown in Fig. 4A. The results in Fig. 4B show agreement between Alice's predictions and Bob's measurements similar to the noncolliding case, $\mathcal{L}_1 = 0.153 \pm 0.012$, and a much larger distance between Alice's classical predictions and Bob's measurements, $\mathcal{L}_1 = 0.995 \pm 0.045$. The latter is expected because two-photon outputs are correspondingly rarer in the classical distribution.

These results confirm that the $n = 2$ and $n = 3$ photon scattering amplitudes are indeed given by the permanents of submatrices generated from U. The small differences, larger for $n = 3$ than $n = 2$, between Alice's Fock-state predictions and Bob's measurement results are expected, because Alice's calculations are for indistinguishable Fock-state inputs, and Bob does not actually have these. The conditioned outputs from downconversion are known to have higher-order terms; that is, a small probability of producing more than one photon per mode [section S5 and fig. S1 (*8*)], and are also spectrally entangled, leading to further distinguishability. Spectrally mismatched detector responses can alter the observed signals because of contributions from the immanent (*12*), of which the determinant and permanent are special cases. Because of flat spectral responses, we can rule this out in our experiment.

Strong evidence against the ECT thesis will come from demonstrating boson sampling with a larger-sized system, in which Bob's experimental sampling is far faster than Alice's calculation and classical verification is still barely possible; according to (*4*), this regime is on the order of $n = 20$ to $n = 30$ photons in a network with $m >> n$ modes. This is beyond current technologies, but rapid improvements in efficient photon detection (*13*, *14*), low-loss (*15*, *16*) and reconfigurable (*17*, *18*) integrated circuits, and improved photon sources (*19*) are highly promising. Boson sampling has also been proposed using the phononic modes of an ion trap (*20*).

An important open question remains as to the practical robustness of large implementations. Unlike the case of universal quantum computation, there are no known error correction protocols for boson sampling, or indeed for any of the models of intermediate quantum computation, such as deterministic quantum computing with one qubit (DQC1) (*21*, *22*), temporally unstructured quantum computation (IQP) (*23*), or permutational quantum computing (PQC) (*24*). These intermediate models have garnered much attention in recent years, both because of the inherent questions they raise about quantum advantage in computing and because some of them can efficiently solve problems believed to be classically intractable; for example, DQC1 has been applied in fields that range from knot theory (*25*) to quantum metrology (*26*). A recent theoretical study posits that photonic boson sampling retains its computational advantage even in the presence of loss (*27*). Our experimental results are highly promising in regard to the robustness of boson sampling, finding good agreement even with clearly imperfect experimental resources.

References and Notes

1. P. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society Press, Los Alamitos, CA, 1994), pp. 124–134.
2. P. C. W. Davies, *Fluct. Noise Lett.* **7**, C37 (2007).
3. L. Valiant, *Theor. Comput. Sci.* **8**, 189 (1979).
4. S. Aaronson, A. Arkhipov, in *Proceedings of the ACM Symposium on Theory of Computing* (ACM, New York, 2011), pp. 333–342.
5. S. Rahimi-Keshari *et al.*, http://arxiv.org/abs/1210.6463 (2012).
6. M. Jerrum, A. Sinclair, E. Vigoda, *J. ACM* **51**, 671 (2004).
7. S. Scheel, http://arxiv.org/pdf/quant-ph/0406127.pdf (2004).
8. Materials and methods are available as supplementary materials on *Science* Online.
9. C. K. Hong, Z. Y. Ou, L. Mandel, *Phys. Rev. Lett.* **59**, 2044 (1987).
10. H. Paul, P. Törmä, T. Kiss, I. Jex, *Phys. Rev. Lett.* **76**, 2464 (1996).
11. P. Kok, S. L. Braunstein, *Phys. Rev. A* **63**, 033812 (2001).
12. S. Tan, Y. Gao, H. de Guise, B. Sanders, http://arxiv.org/abs/1208.5677 (2012).
13. A. E. Lita, A. J. Miller, S. W. Nam, *Opt. Express* **16**, 3032 (2008).
14. D. H. Smith *et al.*, *Nat. Commun.* **3**, 625 (2012).
15. J. O. Owens *et al.*, *New J. Phys.* **13**, 075003 (2011).
16. A. Peruzzo *et al.*, *Science* **329**, 1500 (2010).
17. P. Shadbolt *et al.*, *Nat. Photonics* **6**, 45 (2012).
18. B. Metcalf *et al.*, *Nat. Commun.* **4**, 1365 (2013).
19. A. Dousse *et al.*, *Nature* **466**, 217 (2010).
20. H.-K. Lau, D. F. V. James, *Phys. Rev. A* **85**, 062329 (2012).

21. A. Datta, A. Shaji, C. M. Caves, *Phys. Rev. Lett.* **100**, 050502 (2008).
22. B. P. Lanyon, M. Barbieri, M. P. Almeida, A. G. White, *Phys. Rev. Lett.* **101**, 200501 (2008).
23. M. J. Bremner, R. Jozsa, D. J. Shepherd, *Proc. R. Soc. London Ser. A* **467**, 459 (2011).
24. S. Jordan, *Quantum Inf. Comput.* **10**, 470 (2010).
25. P. Shor, S. Jordan, *Quantum Inf. Comput.* **8**, 681 (2008).
26. S. Boixo, R. D. Somma, *Phys. Rev. A* **77**, 052320 (2008).
27. P. P. Rohde, T. C. Ralph, *Phys. Rev. A* **85**, 022332 (2012).

Acknowledgments: We thank R. Fickler for help with characterization; M. de Almeida, D. Biggerstaff, and G. Gillett for experimental assistance; and A. Arkhipov, M. Bremner, and T. Rudolph for discussions. This work was supported in part by the Australian Research Council's Federation Fellow program (grant FF0668810), the Centre for Engineered Quantum Systems (grant CE110001013), and the Centre for Quantum Computation and Communication Technology (grant CE110001027); the University of Queensland Vice-Chancellor's Senior Research Fellowship program; NSF grant no. 0844626 and a Science and Technology Centre grant; a Defense Advanced Research Projects Agency Young Faculty Award grant; a TIBCO Chair; and a Sloan Fellowship.

Supplementary Materials

www.sciencemag.org/cgi/content/full/science.1231440/DC1
Supplementary Text
Fig. S1
Eqs. S1 to S12
References (*28*–*33*)

12 October 2012; accepted 3 December 2012
Published online 20 December 2012;
10.1126/science.1231440

Boson Sampling on a Photonic Chip

Justin B. Spring,[1]* Benjamin J. Metcalf,[1] Peter C. Humphreys,[1] W. Steven Kolthammer,[1] Xian-Min Jin,[1,2] Marco Barbieri,[1] Animesh Datta,[1] Nicholas Thomas-Peter,[1] Nathan K. Langford,[1,3] Dmytro Kundys,[4] James C. Gates,[4] Brian J. Smith,[1] Peter G. R. Smith,[4] Ian A. Walmsley[1]*

Although universal quantum computers ideally solve problems such as factoring integers exponentially more efficiently than classical machines, the formidable challenges in building such devices motivate the demonstration of simpler, problem-specific algorithms that still promise a quantum speedup. We constructed a quantum boson-sampling machine (QBSM) to sample the output distribution resulting from the nonclassical interference of photons in an integrated photonic circuit, a problem thought to be exponentially hard to solve classically. Unlike universal quantum computation, boson sampling merely requires indistinguishable photons, linear state evolution, and detectors. We benchmarked our QBSM with three and four photons and analyzed sources of sampling inaccuracy. Scaling up to larger devices could offer the first definitive quantum-enhanced computation.

Universal quantum computers require physical systems that are well isolated from the decohering effects of their environment, while at the same time allowing precise manipulation during computation. They also require qubit-specific state initialization, measurement, and generation of quantum correlations across the system (*1*–*4*). Although there has been substantial progress in proof-of-principle demonstrations of quantum computation (*5*–*8*), simultaneously meeting these demands has proven difficult. This motivates the search for schemes that can demonstrate quantum-enhanced computation under more favorable experimental conditions. Investigating the space between classical and universal quantum computers has attracted broad interest (*9*–*11*).

Boson sampling has recently been proposed as a specific quantum computation that is more efficient than its classical counterpart but only requires indistinguishable bosons, low decoherence linear evolution, and measurement (*12*). The distribution of bosons that have undergone a unitary transformation U is thought to be exponentially hard to sample from classically (*12*). The probability amplitude of obtaining a certain output is directly proportional to the permanent of a corresponding submatrix of U (*13*). The permanent expresses the wave function of identical bosons, which are symmetric under exchange (*14*, *15*); in contrast, the Slater determinant expresses the wave function of identical fermions, which are antisymmetric under exchange. Whereas determinants can be evaluated efficiently, permanents have long been believed to be hard to compute (*16*); the best-known algorithm scales exponentially with the size of the matrix.

One can envision a race between a classical and a quantum machine to sample the boson distribution given an input state and U. The classical machine would evaluate at least part of the probability distribution, which requires the analysis of matrix permanents. An ideal quantum boson-sampling machine (QBSM) instead creates indistinguishable bosons, physically implements U, and records the outputs. Although the QBSM is not believed to efficiently estimate any individual matrix permanent, for a sufficiently large system it is expected to beat the classical computer in sampling over the entire distribution (*12*).

Photonics is a natural platform to implement boson sampling because sources of indistinguishable photons are well developed (*17*), and integrated optics offers a scalable route to low decoherence linear transformations over many modes (*18*). Such circuits can be rapidly reconfigured to sample from a user-defined operation (*19*, *20*). Importantly, boson sampling requires neither nonlinearities nor on-demand entanglement, which are substantial challenges in photonic universal quantum computation (*21*). This clears the way for experimental boson sampling with existing photonic technology, building on the extensively studied two-photon Hong-Ou-Mandel interference effect (*22*).

A QBSM (Fig. 1) samples the output distribution of a multiparticle bosonic quantum state $|\Psi_{out}\rangle$, prepared from a specified initial state $|\mathbf{T}\rangle$ and linear transformation Λ. Unavoidable losses in the system imply Λ will not be unitary, although lossy QBSMs can still surpass classical computation (*12*, *23*). A trial begins with the input state $|\mathbf{T}\rangle = |T_1 \ldots T_M\rangle \propto \Pi_{i=1}^{M} (\hat{a}_i^\dagger)^{T_i} |0\rangle$, which describes $N = \sum_{i=1}^{M} T_i$ particles distributed in M input modes in the occupation-number representation. The output state $|\Psi_{out}\rangle$ is generated according to the linear map between input and output mode creation operators $\hat{a}_i^\dagger = \sum_{j=1}^{M} \Lambda_{ij} \hat{b}_j^\dagger$, where $\mathbf{\Lambda}$ is an $M \times M$ matrix. Lastly, the particles in each of the M output modes are counted. The

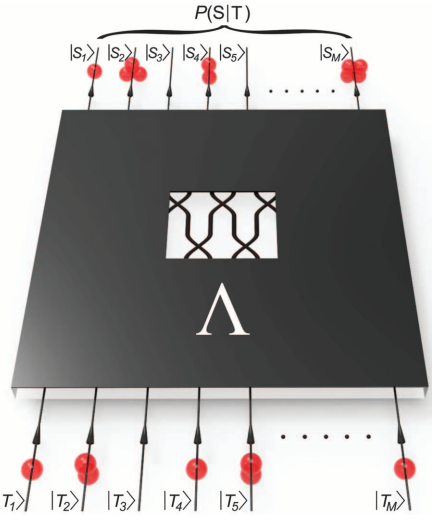

Fig. 1. Model of quantum boson sampling. Given a specified initial number state $|\mathbf{T}\rangle = |T_1 \ldots T_M\rangle$ and linear transformation Λ, a QBSM efficiently samples from the distribution $P(\mathbf{S}|\mathbf{T})$ of possible outcomes $|\mathbf{S}\rangle = |S_1 \ldots S_M\rangle$.

[1]Clarendon Laboratory, Department of Physics, University of Oxford, Oxford OX1 3PU, UK. [2]Department of Physics, Shanghai Jiao Tong University, Shanghai 200240, PR China. [3]Department of Physics, Royal Holloway, University of London, London TW20 0EX, UK. [4]Optoelectronics Research Centre, University of Southampton, Southampton SO17 1BJ, UK.

*To whom correspondence should be addressed. E-mail: j.spring1@physics.ox.ac.uk (J.B.S.); i.walmsley1@physics.ox.ac.uk (I.A.W.)

Science
AAAS

Photonic Boson Sampling in a Tunable Circuit

Matthew A. Broome, Alessandro Fedrizzi, Saleh Rahimi-Keshari, Justin Dove, Scott Aaronson, Timothy C. Ralph and Andrew G. White (December 20, 2012)

Science **339** (6121), 794-798. [doi: 10.1126/science.1231440] originally published online December 20, 2012

Editor's Summary

Computing Power of Quantum Mechanics

There is much interest in developing quantum computers in order to perform certain tasks much faster than, or that are intractable for, a classical computer. A general quantum computer, however, requires the fabrication and operation a number of quantum logic devices (see the Perspective by **Franson**). **Broome *et al.*** (p. 794, published online 20 December) and **Spring *et al.*** (p. 798, published online 20 December) describe experiments in which single photons and quantum interference were used to perform a calculation (the permanent of a matrix) that is very difficult on a classical computer. Similar to random walks, quantum walks on a graph describe the movement of a walker on a set of predetermined paths; instead of flipping a coin to decide which way to go at each point, a quantum walker can take several paths at once. **Childs *et al.*** (p. 791) propose an architecture for a quantum computer, based on quantum walks of multiple interacting walkers. The system is capable of performing any quantum operation using a subset of its nodes, with the size of the subset scaling favorably with the complexity of the operation.

Science (print ISSN 0036-8075; online ISSN 1095-9203) is published weekly, except the last week in December, by the American Association for the Advancement of Science, 1200 New York Avenue NW, Washington, DC 20005.