Sciencexpress Reports

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]

[1]Centre for Engineered Quantum Systems, School of Mathematics and Physics, University of Queensland, Brisbane 4072, Australia. [2]Centre for Quantum Computer,and Communication Technology, School of Mathematics and Physics, University of Queensland, Brisbane 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

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 linear-optical unitary process. Here we test the central premise of boson sampling, experimentally verifying that 3-photon scattering amplitudes are given by the permanents of submatrices generated from a unitary describing a 6-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 will be a much simpler task than building a universal quantum computer.

The key 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 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 like RSA. A third possibility is that the Extended Church-Turing 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 Extended Church-Turing 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, since 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. Note that 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'.

Here we test the central premise of boson sampling, experimentally verifying that the amplitudes of $n = 2$ & $n = 3$ photon scattering events are given by the permanents of $n\times n$ sub-matrices 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, since 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*). Importantly, 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 Extended Church-Turing 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 randomly chosen operator such 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 $\{1,\ldots,6\} = \{|H\rangle_1, |V\rangle_1, |H\rangle_2, |V\rangle_2, |H\rangle_3, |V\rangle_3\}$, where $|H\rangle_1$ is the horizontally polarised 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 characterised the evolution U using the method detailed in section S1 (*8*), and given the input and output configurations $S = (s_1,\ldots,s_m)$ and $T = (t_1,\ldots,t_m)$ 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 $P_T^Q = \left|\mathrm{Per}(U_{ST}\right|^2$. Conversely, the classical scattering probabilities-when the input photons are distinguishable-are given by $P_T^C = \mathrm{Per}(\tilde{U}_{ST})$, where $\tilde{U}_{ST_{ij}} = \left|U_{ST_{ij}}\right|^2$.

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 prepare near-single-photon Fock states via spontaneous parametric downconversion in a nonlinear crystal, Fig. 1C), and for further details 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 non-classical interference visibility instead,

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

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 (*9*). For $n = 3$–where we use three of the photons from a four-photon state–low count rates mean that only three measurements were taken to avoid optical misalignment and 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, $P_T^C(1) = \{-\Delta\tau_\infty, 0, \Delta\tau_\infty\}$ and $P_T^C(2) = \{\Delta\tau_\infty, 0, -\Delta\tau_\infty\}$, 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 are 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,

$$\mathcal{L}_1 = \frac{1}{C(m,n)} \Sigma_T \left|V_T^A - V_T^B\right|$$

where $C(m,n)$ is the binomial coefficient, see 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—e.g. coherent states from a laser, see 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 to Bob's quantum measurements, with $\overline{\mathcal{L}}_1 = 0.548 \pm 0.006$. This large, statistically significant, disagreement highlights 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 compared with the two-photon case, see section S5 (*8*). Having tested all possible `non-colliding' 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) shows agreement between Alice's predictions and Bob's measurements similar to the non-colliding case, $\overline{\mathcal{L}}_1 = 0.153 \pm 0.012$, and a much larger distance between Alice's classical predictions and Bob's measurements, $\overline{\mathcal{L}}_1 = 0.995 \pm 0.045$. The latter is expected as 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, since 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, i.e., a small probability of producing more than one-photon per mode-see section S5 and fig. S1 (*8*)-and are also spectrally entangled, leading to further distinguishability. Interestingly, spectrally mismatched detector responses can alter the observed signals due to contributions from the immanent (*12*), of which the determinant and permanent are special cases. Due to flat spectral responses, we can rule this out in our experiment.

Strong evidence against the Extended Church-Turing thesis will come from demonstrating boson sampling with a larger-sized system where Bob's experimental sampling is far faster than Alice's calculation and where 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 be 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 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 due both to the inherent questions they raise about quantum advantage in computing, and because some of them can efficiently solve problems believed to be classically intractable, e.g., 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, *Proc. 35th Ann. Symp. Found. Comp. Sci.* (IEEE Comp. Soc. Press) (1994).
2. P. C. W. Davies, The implications of a cosmological information bound for complexity, quantum information and the nature of physical law. *Fluct. Noise Lett.* **7**, C37 (2007). doi:10.1142/S0219477507004021
3. L. Valiant, The complexity of computing the permanent. *Theor. Comput. Sci.* **8**, 189 (1979). doi:10.1016/0304-3975(79)90044-6
4. S. Aaronson, A. Arkhipov, Proc. ACM Symposium on Theory of Computing, San Jose, CA, pp. 333–342 (2011).
5. S. Rahimi-Keshari *et al*., arXiv:1210.6463 (2012).
6. M. Jerrum, A. Sinclair, E. Vigoda, A polynomial-time approximation algorithm for the permanent of a matrix with nonnegative entries. *J. ACM* **51**, 671 (2004). doi:10.1145/1008731.1008738

7. S. Scheel, arXiv:quant-ph/0406127v1 (2004).
8. Materials and methods are available as supplementary materials on *Science* Online.
9. C. K. Hong, Z. Y. Ou, L. Mandel, Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.* **59**, 2044 (1987). doi:10.1103/PhysRevLett.59.2044 Medline
10. H. Paul, P. Törmä, T. Kiss, I. Jex, Photon chopping: New way to measure the quantum state of light. *Phys. Rev. Lett.* **76**, 2464 (1996). doi:10.1103/PhysRevLett.76.2464 Medline
11. P. Kok, S. L. Braunstein, Detection devices in entanglement-based optical state preparation. *Phys. Rev. A* **63**, 033812 (2001). doi:10.1103/PhysRevA.63.033812
12. S. Tan, Y. Gao, H. de Guise, B. Sanders, arXiv preprint arXiv:1208.5677 (2012).
13. A. E. Lita, A. J. Miller, S. W. Nam, Counting near-infrared single-photons with 95% efficiency. *Opt. Express* **16**, 3032 (2008). doi:10.1364/OE.16.003032 Medline
14. D. H. Smith *et al*., Conclusive quantum steering with superconducting transition-edge sensors. *Nature Communications* **3**, 625 (2012). doi:10.1038/ncomms1628 Medline
15. J. O. Owens *et al*., Two-photon quantum walks in an elliptical direct-write waveguide array. *New J. Phys.* **13**, 075003 (2011). doi:10.1088/1367-2630/13/7/075003
16. A. Peruzzo *et al*., Quantum walks of correlated photons. *Science* **329**, 1500 (2010). doi:10.1126/science.1193515 Medline
17. P. Shadbolt *et al*., Generating, manipulating and measuring entanglement and mixture with a reconfigurable photonic circuit. *Nat. Photonics* **6**, 45 (2012). doi:10.1038/nphoton.2011.283
18. B. Metcalf *et al*., arXiv:1208.4575 (2012).
19. A. Dousse *et al*., Ultrabright source of entangled photon pairs. *Nature* **466**, 217 (2010). doi:10.1038/nature09148 Medline
20. H.-K. Lau, D. F. V. James, Proposal for a scalable universal bosonic simulator using individually trapped ions. *Phys. Rev. A* **85**, 062329 (2012). doi:10.1103/PhysRevA.85.062329
21. A. Datta, A. Shaji, C. M. Caves, Quantum discord and the power of one qubit. *Phys. Rev. Lett.* **100**, 050502 (2008). doi:10.1103/PhysRevLett.100.050502 Medline
22. B. P. Lanyon, M. Barbieri, M. P. Almeida, A. G. White, Experimental quantum computing without entanglement. *Phys. Rev. Lett.* **101**, 200501 (2008). doi:10.1103/PhysRevLett.101.200501 Medline
23. M. J. Bremner, R. Jozsa, D. J. Shepherd, Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science **467**, 459 (2011).
24. S. Jordan, Quantum Information & Computation **10**, 470 (2010).
25. P. Shor, S. Jordan, *Quantum Information & Computation* **8**, 681 (2008).
26. S. Boixo, R. D. Somma, Parameter estimation with mixed-state quantum computation. *Phys. Rev. A* **77**, 052320 (2008). doi:10.1103/PhysRevA.77.052320
27. P. P. Rohde, T. C. Ralph, Error tolerance of the boson-sampling model for linear optics quantum computing. *Phys. Rev. A* **85**, 022332 (2012). doi:10.1103/PhysRevA.85.022332
28. J. L. O'Brien *et al*., Quantum process tomography of a controlled-NOT gate. *Phys. Rev. Lett.* **93**, 080502 (2004). doi:10.1103/PhysRevLett.93.080502 Medline
29. A. Laing, J. L. O'Brien, arXiv:1208.2868 (2012).
30. L. Mandel, Photon interference and correlation effects produced by independent quantum sources. *Phys. Rev. A* **28**, 929 (1983). doi:10.1103/PhysRevA.28.929
31. M. A. Broome, M. P. Almeida, A. Fedrizzi, A. G. White, Reducing multi-photon rates in pulsed down-conversion by temporal multiplexing. *Opt. Express* **19**, 22698 (2011). doi:10.1364/OE.19.022698 Medline
32. X. Yao *et al*., Observation of eight-photon entanglement. *Nat. Photonics* **6**, 225 (2012). doi:10.1038/nphoton.2011.354
33. X. Ma, S. Zotter, J. Kofler, T. Jennewein, A. Zeilinger, Experimental generation of single photons via active multiplexing. *Phys. Rev. A* **83**, 043814 (2011). doi:10.1103/PhysRevA.83.043814

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 (FF0668810), Centre for Engineered Quantum Systems (CE110001013), and Centre for Quantum Computation and Communication Technology (CE110001027); the University of Queensland Vice-Chancellor's Senior Research Fellowship program; the National Science Foundation's grant no. 0844626, and a Science and Technology Centre grant; a DARPA 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

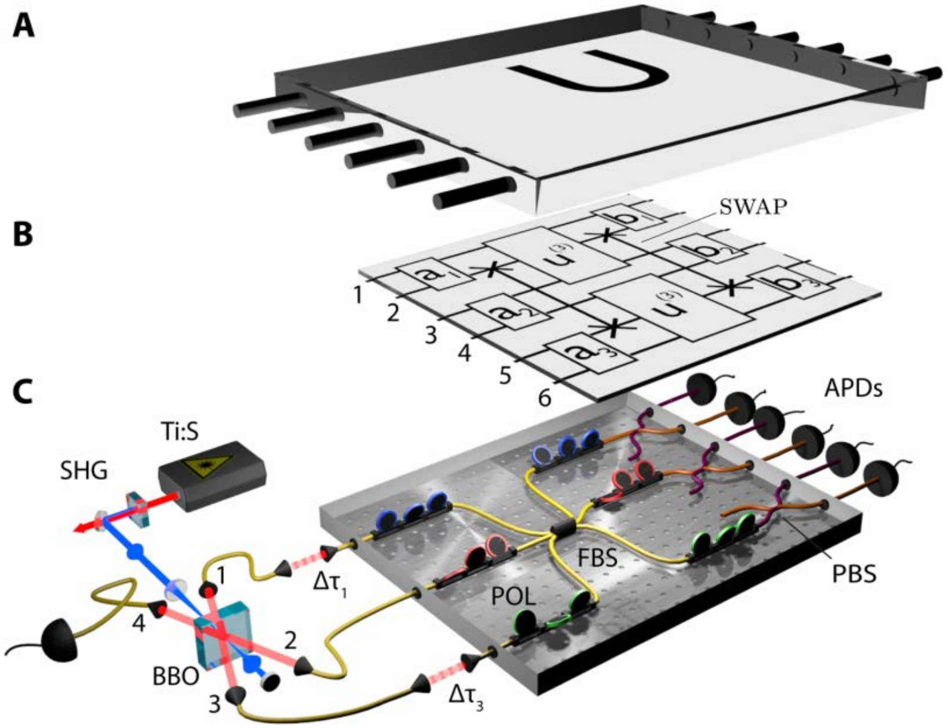

Fig. 1. Experimental scheme for boson sampling. (**A**) Both Alice and Bob-possessing classical and quantum resources respectively-must sample the output distribution from some unitary, U. (**B**) Equivalent circuit: The orthogonal polarizations in each input spatial mode can be arbitrarily combined by the unitaries $a_1 . . . a_3$. A multi-port, $u^{(3)}$, interferes all modes of the same polarization; orthogonal polarizations are recombined by $b_1 . . . b_3$. (**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, photons 1-3 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, $a_1 . . . b_3$ are implemented with polarization controllers (POL); $u^{(3)}$ is implemented by a 3×3 non-polarising fiber beam-splitter (FBS); three polarising fiber beam-splitters (PBS) output 6 spatial modes to single photon avalanche diodes (APDs). The fiber beam-splitters work by evanescent coupling between multiple input fibers in close proximity.

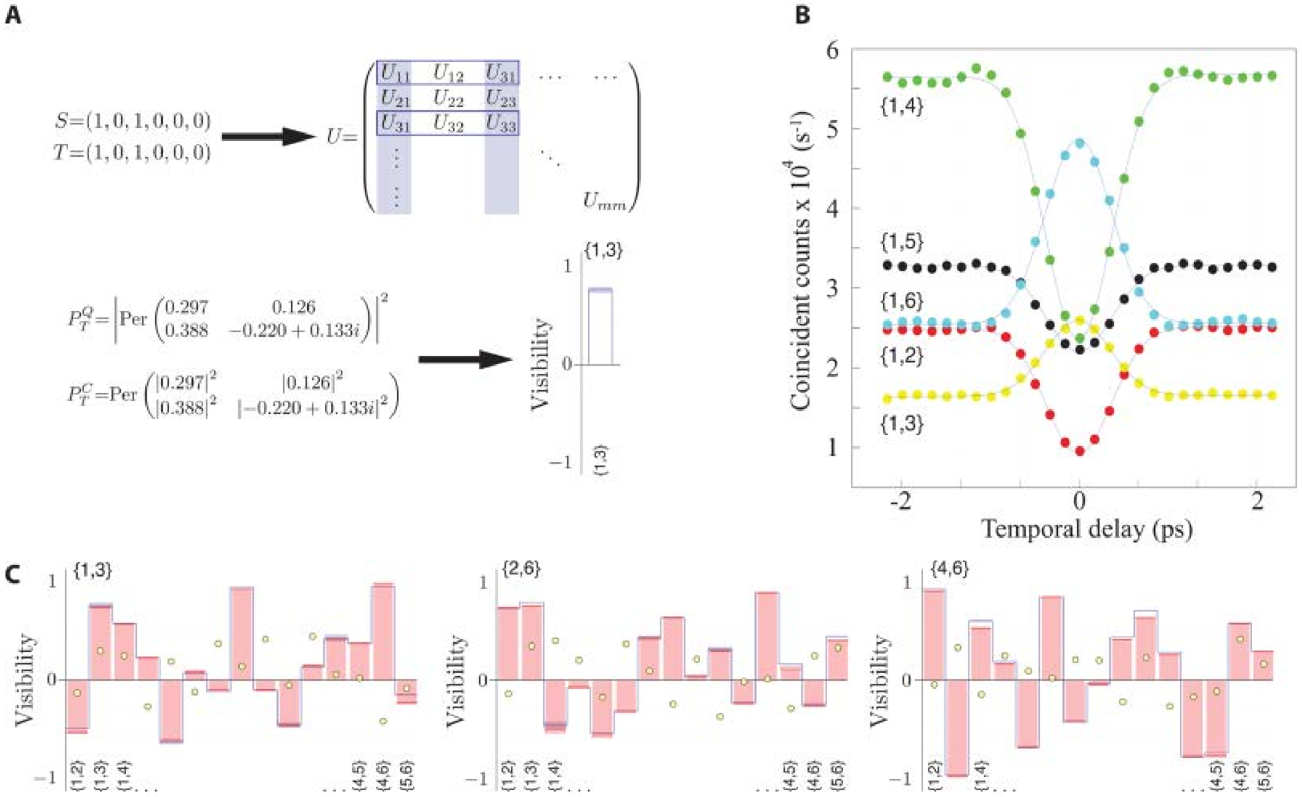

Fig. 2. Two-photon boson sampling. (**A**) Outline of Alice's technique to predict visibilities from the unitary evolution *U* (*8*). For photons input and output in modes 1 and 3 her prediction give by the bar (bottom-right); its uncertainty-obtained by 10 separate characterizations of the unitary-is represented by the shaded box on top of 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) two-photon visibilities. Input configurations are shown top-left of each panel; output modes are labeled at plot bottom. Errors are given by light-blue and dark-red boxes at the extrema of each data set. Yellow circles are the visibility predictions given coherent input-states.

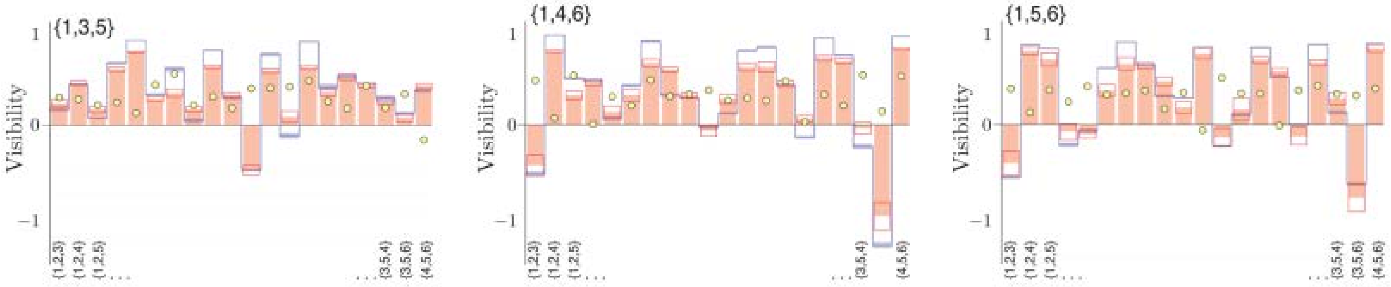

Fig. 3. Three-photon boson sampling. Alice's predictions (blue line envelope) and Bob's measurements (orange bars) for three-photon visibilities. Labels, errors, and symbols are as defined in Fig. 2C).

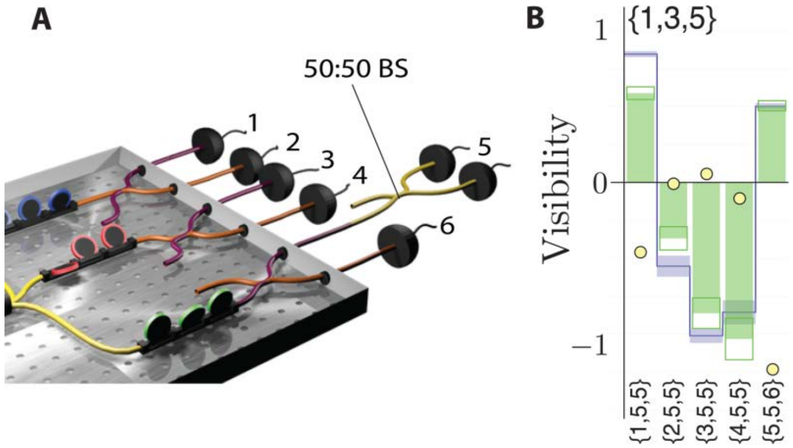

Fig. 4. Three-photon boson sampling with colliding outputs. (**A**) Number-resolution was achieved with a 50:50 fiber beam-splitter in mode 5 and an additional detector. Note that an imperfect splitting ratio for this FBS impedes only the effective efficiency of our number resolving scheme (*10*, *11*). (**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)