Optical Quantum Computing
Jeremy L. O'Brien
Science **318**, 1567 (2007);
DOI: 10.1126/science.1142892

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.

Optical Quantum Computing

Jeremy L. O'Brien

In 2001, all-optical quantum computing became feasible with the discovery that scalable quantum computing is possible using only single-photon sources, linear optical elements, and single-photon detectors. Although it was in principle scalable, the massive resource overhead made the scheme practically daunting. However, several simplifications were followed by proof-of-principle demonstrations, and recent approaches based on cluster states or error encoding have dramatically reduced this worrying resource overhead, making an all-optical architecture a serious contender for the ultimate goal of a large-scale quantum computer. Key challenges will be the realization of high-efficiency sources of indistinguishable single photons, low-loss, scalable optical circuits, high-efficiency single-photon detectors, and low-loss interfacing of these components.

Over the last few decades quantum information science has emerged to consider what additional power and functionality can be realized in the encoding, transmission, and processing of information by specifically harnessing quantum mechanical effects (*1*). Anticipated technologies include quantum key distribution (*2*), which offers perfectly secure communication; quantum metrology (*3*), which allows more precise measurements than could ever be achieved without quantum mechanics; and quantum lithography (*4*), which could enable fabrication of devices with features much smaller than the wavelength of light. Perhaps the most startling and powerful future quantum technology is a quantum computer, which promises exponentially faster computation for particular tasks (*1*, *5*).

The quest to develop a quantum computer will require formidable technical mastery of the fabrication of devices at the nano and possibly atomic scale, and precision control of their quantum mechanical states. The task is also daunting owing to the inherent fragility of quantum states and the fact that quantum entanglement, and its role in a quantum computer, is not yet fully understood. As we engineer devices that exploit quantum mechanical effects, we will gain an unprecedented control over the fundamental workings of nature as well as a deeper understanding of them.

The requirements for realizing a quantum computer are confounding: scalable physical qubits—two-state quantum systems—that can be well isolated from the environment but also initialized, measured, and controllably interacted to implement a universal set of quantum logic gates (*6*). However, a number of physical implementations are being pursued, including nuclear magnetic resonance, ion, atom, cavity quantum electrodynamics, solid state, and superconducting systems (*7*). Over the past few years, single particles of light—photons—have emerged as a leading approach.

Centre for Quantum Photonics, H. H. Wills Physics Laboratory and Department of Electrical and Electronic Engineering, University of Bristol, Merchant Venturers Building, Woodland Road, Bristol, BS8 1UB, UK.

E-mail: Jeremy.OBrien@bristol.ac.uk

Single Photons as Qubits

Single photons are largely free of the noise, or decoherence, that plagues other systems; can be easily manipulated to realize one-qubit logic gates; and enable encoding in any of several degrees of freedom, for example, polarization, time bin, or path. Figure 1A shows how a qubit can be encoded in the polarization of a single photon. An arbitrary state of a single qubit $\alpha|H\rangle + \beta|V\rangle$ ($|\alpha|^2 + |\beta|^2 = 1$) can be represented on the Poincaré (or Bloch) sphere (Fig. 1B). One-qubit logic gates are straightforward, using birefringent wave plates (Fig. 1C), and converting between polarization and path encoding can be easily achieved using a polarizing beam splitter (PBS) (Fig. 1D), where $|0\rangle$ or $|1\rangle$ now represents a photon in the upper or lower path, respectively.

A major difficulty for optical quantum computing is in realizing the entangling logic gates required for universal quantum computation. The canonical example is the controlled NOT gate (CNOT), which flips the state of a target (T) qubit conditional on a control (C) qubit being in the logical state "1." Figure 2A shows why this operation is difficult. The two paths used to encode the target qubit are mixed at a 50% reflecting beam splitter (BS) (or half-silvered mirror), which performs the Hadamard operation (Fig. 1C). If the phase shift is not applied, the second Hadamard (BS) undoes the first, returning the target qubit to exactly the same state it started in (this is an example of "classical" wave interference). If, however, a (π) phase shift is applied, that is, $|0\rangle + |1\rangle \leftrightarrow |0\rangle - |1\rangle$, the target qubit undergoes a bit-flip or NOT operation. A CNOT must implement this phase shift only if the control photon is in the "1" path. No known or foreseen material has an optical nonlinearity strong enough to implement this conditional phase shift [although tremendous progress has been made with single atoms in high-finesse optical cavities (*8*–*10*)].

In 2001, a major breakthrough showed that scalable quantum computing is possible using

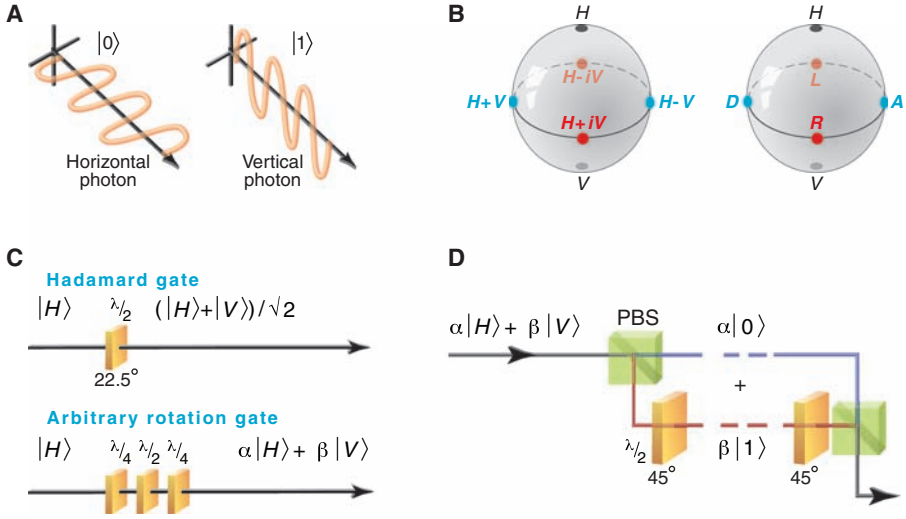

Fig. 1. Single-photon qubits. (**A**) A horizontal (H) photon represents a logical "0" and a vertical (V) photon represents a logical "1": $|0\rangle \equiv |H\rangle$; $|1\rangle \equiv |V\rangle$. (**B**) An arbitrary state can be plotted on the Bloch (or Poincaré) sphere. Examples of diagonal ($|D\rangle \equiv |0\rangle+|1\rangle$), antidiagonal ($|A\rangle \equiv |0\rangle-|1\rangle$), right circular ($|R\rangle \equiv |0\rangle+i|1\rangle$), and left circular ($|L\rangle \equiv |0\rangle-i|1\rangle$) are shown. (**C**) Single-qubit gates are easily realized using birefringent wave plates that retard one polarization by a fraction of a wavelength λ relative to an orthogonal polarization, causing a rotation of the state on the Bloch sphere, with the axis of rotation determined by the orientation of the wave plate. For example, a Hadamard (H) gate (defined by its operation on the logical states: $|0\rangle \rightarrow |0\rangle+|1\rangle$; $|1\rangle \rightarrow |0\rangle-|1\rangle$ or $|H\rangle \rightarrow |D\rangle$; $|V\rangle \rightarrow |A\rangle$) causes a π rotation about an axis running through the midpoint between the $|H\rangle$ and $|D\rangle$ states and can be realized by a $\lambda/2$ wave plate oriented at 22.5°. An arbitrary rotation requires a $\lambda/4$-$\lambda/2$-$\lambda/4$ sequence. (**D**) Converting between polarization and path encoding requires a PBS, which transmits *H* and reflects *V*, and a $\lambda/2$ wave plate oriented at 45°, which transforms $|V\rangle \leftrightarrow |H\rangle$.

only single-photon sources and detectors and simple (linear) optical circuits consisting of BSs (*11*). This is a truly remarkable discovery, because the argument above suggests that a strong optical nonlinearity is required to realize the most basic logic element.

Linear Optical Quantum Computing

A diagram of a nondeterministic (probabilistic with success signal) CNOT is shown in Fig. 3C. The control and target qubits (encoded in polarization, say), together with two auxiliary photons, enter an optical network of BSs, where the four photons' paths are combined. At the output of this network, the control and target photons emerge, having had the CNOT logic operation applied to their state, conditional on a single photon being detected at both detectors. This detection event occurs with probability $P < 1$ (1/16 in the original scheme); the rest of the time ($P = 15/16$), another detection pattern is recorded (none, only one, two photons at one detector, and so on) and the CNOT logic is not applied. In fact, a single photon may not even emerge from the control and/or target outputs in these cases.

A nondeterministic CNOT is of little use for quantum computing because the probability that a computation succeeds decreases exponentially with the number of CNOTs. Fortunately, the success probability of the nondeterministic CNOT can be boosted by harnessing quantum teleportation (*12*), a process whereby the unknown state of a qubit can be transferred to another qubit. The idea is to teleport a nondeterministic gate that has already worked onto the control and target qubits (*13*) (Fig. 3). Quantum teleportation has been realized with single photons (*14*).

An important omission from the above discussion is that, because the Bell measurements required for teleportation (Fig. 3B) measure maximally entangled states, they require a similar optical nonlinearity as a CNOT (although the photons can be destroyed in the measurement) and therefore fail some of the time. When they fail, they measure the state of the control and target photons in the $\{|0\rangle,|1\rangle\}$ basis. The final component is an encoding against this "measurement error": A single logical qubit is encoded in several physical qubits such that if one of the physical qubits is measured, the original logical qubit can still be recovered. These encoded states are entangled and therefore require entangling gates to realize them. However, by using more and more photons, a CNOT with a probability of success approaching 1 can be realized (*11*).

Reducing the Resource Overhead

These developments were expanded upon (*15*–*19*) and soon followed by several proof-of-principal experimental demonstrations of CNOTs (*20*–*23*) and encoding against measurement error (*24*, *25*). Despite this great progress, optical quantum computing was still widely regarded as impractical owing to the large resource overhead required to realize a near-deterministic CNOT: >10,000 pairs of entangled photons to achieve a success probability of >95%. The reason that all-optical quantum computing is today a promising route to practical quantum computing is due to new schemes that dramatically reduce this worrying resource overhead.

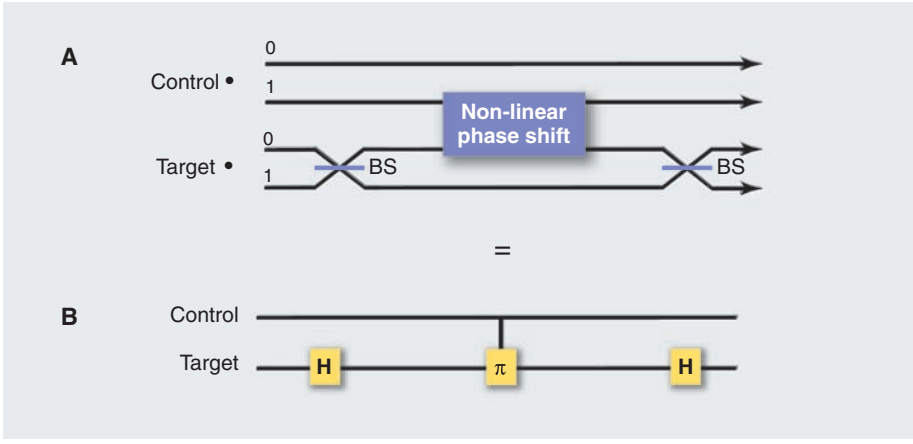

Fig. 2. An optical CNOT gate. (**A**) Schematic of a possible realization of an optical CNOT gate. (**B**) In the notation of quantum circuits, the BSs each implement a Hadamard (H) gate.

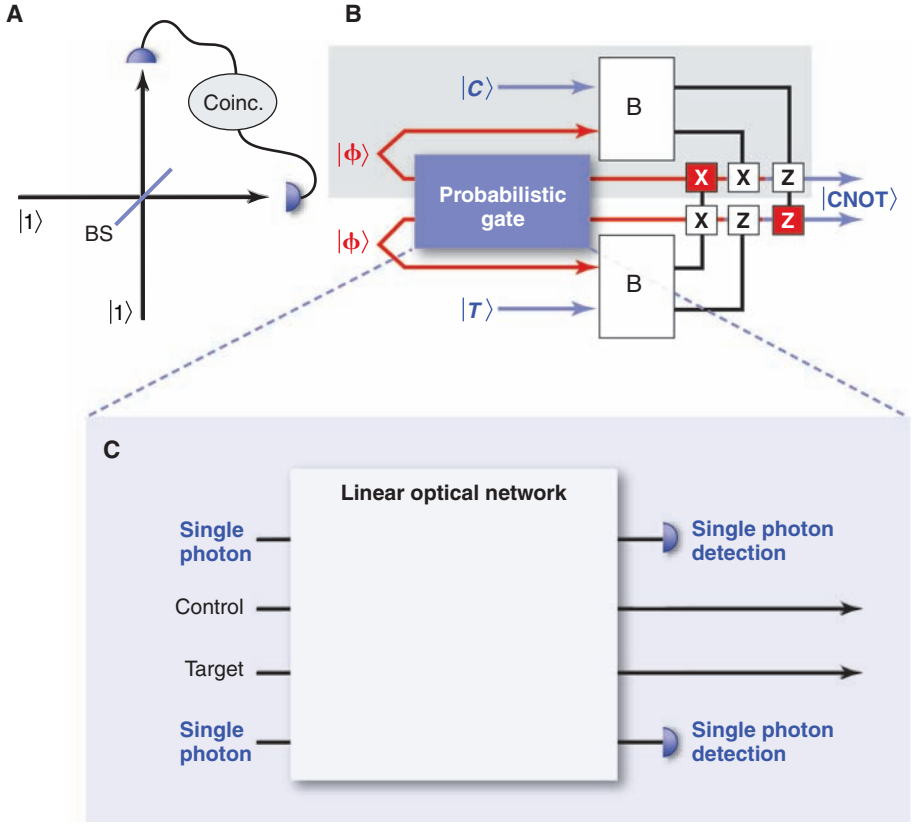

Fig. 3. An optical CNOT gate by teleportation. (**A**) Quantum interference of two photons at a BS. (**B**) Teleportation of a CNOT. Ignoring the Probabilistic Gate, a qubit in an unknown state $|C\rangle$ and one of two photons prepared in a maximally entangled state $|\phi\rangle$ are subjected to a Bell measurement (B). This measurement leaves the third qubit in the state $|C\rangle$, or the bit (X), and/or phase (Z) flipped version of $|C\rangle$, depending on which of the four maximally entangled states is measured. An unwanted X and/or Z flip can be trivially corrected by applying a second X and/or Z as required. Still ignoring the Probabilistic Gate, the unknown input state of the control and target qubits can both be teleported and the CNOT performed on the output qubits. This seems like a lot of extra work for no gain; however, performing the CNOT before the (possible) X and Z flip has the tremendous advantage that we could repeatedly attempt the CNOT on the two halves of two entangled states, and only when the gate works would we proceed with teleportation. In this way, the control and target qubits are preserved until the gate works (on average, 32 entangled states will be consumed) and we can implement the CNOT deterministically. In quantum mechanics, the order in which operations are performed is important; performing the CNOT earlier means we must add the X and Z flips indicated in red (*13*). (**C**) A diagram of a measurement-assisted nondeterministic CNOT gate.

Quantum computations (regardless of physical realization) are typically formulated using the quantum circuit model (e.g., Fig. 2B), a generalization of the circuit model for Boolean logic: Qubits are represented by wires propagating in time from left to right, subjected to a sequence of quantum logic gates, and finally measured (*1*). In 2001 a remarkable alternative was proposed in which the computation starts with a particular massively entangled state of many qubits (a cluster state) and the computation proceeds by a sequence of single-qubit measurements, from left to right, that ultimately leave the rightmost column of qubits in the answer state (*26*) (Fig. 4).

In 2004, it was recognized that the cluster approach offered tremendous advantages for optical realizations (*27*) [see also (*28*)]. Because preparation of the cluster state can be probabilistic, nondeterministic CNOTs are suitable for making it, removing much of the massive overhead that arises from the error encoding used to make near-deterministic CNOTs. It turns out that a similar advantage can also be gained in the circuit formulation of optical quantum computing by using more sophisticated error-encoding techniques (*29*). These, and other techniques that dispense with CNOT gates entirely (*30*), reduce the resources required by 3 to 4 orders of magnitude, making an all-optical approach far more attractive. There have already been experimental proof-of-principle demonstrations of these new schemes [e.g., (*31*–*34*)].

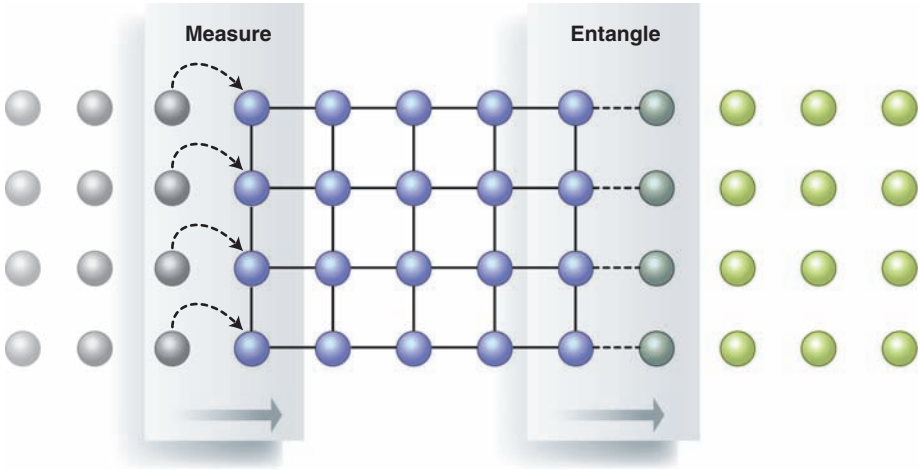

Fig. 4. Cluster state quantum computing. For photons, it is practical to start measuring the qubits while the cluster is still being grown. The blue qubits are in a cluster state, where the bonds between them represent entanglement. The green qubits are being added to the cluster, whereas the gray qubits have been measured and are no longer entangled. The measurement outcome determines the basis for the measurement on the next qubit.

Fault Tolerance

The final, and arguably most important, consideration (for all physical realizations) is fault tolerance (*1*). In contrast to conventional computers, quantum computers will be very susceptible to noise, which must be encoded against (in addition to the encoding described above). The threshold theorem says that if the noise is below some threshold, an arbitrarily long quantum computation can be realized. One of the most encouraging results for all approaches to quantum computing was the high threshold of 1% recently reported by Knill (*35*). Because cluster state approaches do not conform to the standard model, the threshold theorem does not apply; fortunately, analogous thresholds have been shown to exist (*36*). Recent results give cause for optimism: They show that if the product of source and detector efficiency is >2/3, then optical quantum computing is possible, provided all other components operate perfectly (*37*) (photon loss can in some cases be incorporated into source or detector efficiency). More complete treatments that consider more sources of noise give thresholds of 10^{-3} to 10^{-4} (*38*). The true number will likely lie somewhere in between.

Sources, Detectors, and Circuits

There are very stringent requirements for single-photon sources for optical quantum computing. In a general linear optical network (e.g., Fig. 3C) there are places where photons arrive at both inputs to a BS where quantum interference of two (or more) photons can occur. An example is shown in Fig. 3A where a photon enters each input of a 50% reflective BS. The probability of detecting a single photon at each output is given by the square of the sum of the probability amplitude for both photons to be transmitted and that for both photons to be reflected: $P = |r.r + t.t|^2$. Because a phase shift occurs on reflection $r.r = -t.t$ and so $P = 0$, in contrast to our (classical) expectation: $P = 1/2$ (*39*). For quantum interference to occur, the two photons must be indistinguishable from one another in all degrees of freedom.

To date, small-scale tests of optical quantum computing have relied on indistinguishable pairs of photons generated by a strong laser pulse in a nonlinear crystal. Unfortunately, this process is spontaneous and not readily scalable (*40*). Solid-state sources of single photons hold the promise of ready integration, and quantum interference between subsequent photons emitted from a semiconductor quantum dot has been observed (*41*). However, an optical quantum computer will require quantum interference between photons emitted from independent sources. This has very recently been achieved for a pair of trapped atoms (*42*) and ions (*43*), a tremendous advance that bodes well for optical quantum computing. Impurities in diamond may offer the best of both worlds—a solid-state host and atom-like energy levels—and have emerged as very promising candidates (*40*).

It is actually the inherent nonlinearity of photon measurement, combined with quantum interference of photons, that makes linear optical quantum computing possible. Single-photon counting modules are commercially available and have been used for almost all demonstrations to date; however, they cannot distinguish between one or more photons and have a limited efficiency (~70%). Higher efficiency will be required for scalable optical quantum computing, whereas photon number resolution will be desirable. Ongoing work indicates that such high-performance detectors will become available, with superconductor-based devices holding great promise (*44*).

Finally, almost all demonstrations of linear optical logic circuits have relied on large-scale BSs and mirrors, with photons propagating in air; improved performance, miniaturization, and scalability will likely require low-loss microscopic optical waveguide circuits. A promising approach is integrated optics, an analog of electrical integrated circuits, which has been developed by the photonics industry. Outstanding challenges are to realize quantum interference in these devices and to integrate them with single-photon sources and detectors.

Nonlinear and Hybrid Approaches

Recently, attention has been given to the idea of combining linear optics with optical nonlinearities that would not allow a CNOT gate to be realized in the manner suggested in Fig. 2 but would nevertheless offer considerable advantages. One way is to use a two-photon absorber to implement the quantum Zeno effect, whereby repeated measurement inhibits the emission of two photons into one of the outputs of a CNOT gate (*45*)—the failure mode of the linear optical CNOT gate proposed in (*16*). Another way is to use a strong optical nonlinearity that is significantly weaker than that required in Fig. 2: Single photons are made to interact with one another by means of a bright laser pulse and the nonlinear medium (*46*). Finally, recent developments suggest that a hybrid approach may have many advantages (*47*–*50*): Because single-photon sources are inherently quantum mechanical, it is prom-

ising to consider storing quantum information in the sources themselves; already, spins associated with impurities in diamond have shown great promise in this direction (*51*). Such systems are particularly suited to the small-scale quantum processors that will be required in the nodes and quantum repeaters of quantum communication networks (*52*).

Future Prospects

Despite great progress, much work remains to be done if a large-scale optical quantum computer is to be realized. It is not yet known whether the circuit or cluster model (or some other approach) is most promising. Indeed, a combination of these approaches has been described in which error encoding is achieved using cluster techniques but the computation proceeds through conventional CNOT gates (*53*). Further, the role of nonlinear optics approaches in any future optical quantum computer will depend on their efficacy and practicality. The majority of experimental demonstrations to date have relied on nonscalable single-photon sources, large-scale optical elements, and modest-efficiency single-photon detectors. Scaling to useful devices will require high-efficiency single-photon sources and detectors that are efficiently coupled to low-loss microscopic optical waveguide circuits [optical memories may not be required (*54*)].

References and Notes

1. M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge Univ. Press, 2000).
2. N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, *Rev. Mod. Phys.* **74**, 145 (2002).
3. V. Giovannetti, S. Lloyd, L. Maccone, *Science* **306**, 1330 (2004).
4. A. N. Boto *et al*., *Phys. Rev. Lett.* **85**, 2733 (2000).
5. D. Deutsch, *Proc. R. Soc. Lond. A* **400**, 97 (1985).
6. D. P. DiVincenzo, D. Loss, *Superlatt. Micro.* **23**, 419 (1998).
7. See the U.S. Advanced Research and Development Activity (ARDA) Quantum Computation Roadmap for current state-of-the-art; http://qist.lanl.gov/qcomp_map.shtml.
8. Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi, H. J. Kimble, *Phys. Rev. Lett.* **75**, 4710 (1995).
9. T. Aoki *et al*., *Nature* **443**, 671 (2006).
10. M. Hijlkema *et al*., *Nature Phys.* **3**, 253 (2007).
11. E. Knill, R. Laflamme, G. J. Milburn, *Nature* **409**, 46 (2001).
12. C. H. Bennett *et al*., *Phys. Rev. Lett.* **70**, 1895 (1993).
13. D. Gottesman, I. L. Chuang, *Nature* **402**, 390 (1999).
14. D. Bouwmeester *et al*., *Nature* **390**, 575 (1997).
15. M. Koashi, T. Yamamoto, N. Imoto, *Phys. Rev. A* **63**, 030301 (2001).
16. T. B. Pittman, B. C. Jacobs, J. D. Franson, *Phys. Rev. A* **64**, 062311 (2001).
17. T. C. Ralph, A. G. White, W. J. Munro, G. J. Milburn, *Phys. Rev. A* **65**, 012314 (2001).
18. T. C. Ralph, N. K. Langford, T. B. Bell, A. G. White, *Phys. Rev. A* **65**, 062324 (2001).
19. H. F. Hofmann, S. Takeuchi, *Phys. Rev. A* **66**, 024308 (2001).
20. T. B. Pittman, M. J. Fitch, B. C. Jacobs, J. D. Franson, *Phys. Rev. A* **68**, 032316 (2003).
21. J. L. O'Brien, G. J. Pryde, A. G. White, T. C. Ralph, D. Branning, *Nature* **426**, 264 (2003).
22. J. L. O'Brien *et al*., *Phys. Rev. Lett.* **93**, 080502 (2004).
23. S. Gasparoni, J.-W. Pan, P. Walther, T. Rudolph, A. Zeilinger, *Phys. Rev. Lett.* **93**, 020504 (2004).
24. J. L. O'Brien, G. J. Pryde, A. G. White, T. C. Ralph, *Phys. Rev. A* **71**, 060303 (2005).
25. T. B. Pittman, B. C. Jacobs, J. D. Franson, *Phys. Rev. A* **71**, 052332 (2005).
26. R. Raussendorf, H. J. Briegel, *Phys. Rev. Lett.* **86**, 5188 (2001).
27. M. A. Nielsen, *Phys. Rev. Lett.* **93**, 040503 (2004).
28. N. Yoran, B. Reznik, *Phys. Rev. Lett.* **91**, 037903 (2003).
29. T. C. Ralph, A. J. F. Hayes, A. Gilchrist, *Phys. Rev. Lett.* **95**, 100501 (2005).
30. D. E. Browne, T. Rudolph, *Phys. Rev. Lett.* **95**, 010501 (2005).
31. P. Walther *et al*., *Nature* **434**, 169 (2005).
32. N. Kiesel *et al*., *Phys. Rev. Lett.* **95**, 210502 (2005).
33. R. Prevedel *et al*., *Nature* **445**, 65 (2007).
34. C.-Y. Lu *et al*., *Nat. Phys.* **3**, 91 (2007).
35. E. Knill, *Nature* **434**, 39 (2005).
36. M. A. Nielsen, C. M. Dawson, *Phys. Rev. A* **71**, 042323 (2005).
37. M. Varnava, D. Browne, T. Rudolph, *arXiv:quant-ph/0702044* (2007).
38. C. M. Dawson, H. L. Haselgrove, M. A. Nielsen, *Phys. Rev. A* **73**, 052306 (2006).
39. Quantum mechanics tells us that if a particular event can happen in two or more indistinguishable ways, we must first sum the probability amplitudes before squaring to obtain a probability. Because these amplitudes can be negative, it is possible for events that we would intuitively expect to be possible to have zero probability. If the BS is more or less reflective than 50%, these two amplitudes no longer have the same magnitude but are still opposite in sign, meaning that the probability is nonzero but less than one would naively expect.
40. See special issue: Focus on Single Photons on Demand, Eds., P. Grangier, B. Sanders, and J. Vuckovic, *New J. Phys.* **6** (2004).
41. C. Santori, D. Fattal, J. Vuckovic, G. S. Solomon, Y. Yamamoto. *Nature* **419**, 594 (2002).
42. J. Beugnon *et al*., *Nature* **440**, 779 (2007).
43. P. Maunz *et al*., *Nat. Phys.* **3**, 538 (2007).
44. See special issue: Single-photon: detectors, applications, and measurement methods, Eds., A. Migdal and J. Dowling, *J. Mod. Opt.* **51** (2004).
45. J. D. Franson, B. C. Jacobs, T. B. Pittman, *Phys. Rev. A* **70**, 062302 (2004).
46. S. D. Barrett *et al*., *Phys. Rev. A* **71**, 060302 (2005).
47. D. E. Browne, M. B. Plenio, S. F. Huelga, *Phys. Rev. Lett.* **91**, 067901 (2003).
48. S. C. Benjamin, J. Eisert, T. M. Stace, *New J. Phys.* **7**, 194 (2005).
49. Y.-L. Lim, S. D. Barrett, A. Beige, P. Kok, L. C. Kwek, *Phys. Rev. A* **73**, 012304 (2006).
50. S. J. Devitt *et al*., *Phys. Rev. A* **76**, 052312 (2007).
51. F. Jelezko, J. Wrachtrup, *J. Phys. Condens. Matt.* **16**, 1089 (2004).
52. L. Childress, J. M. Taylor, A. Sørensen, M. D. Lukin, *Phys. Rev. Lett.* **96**, 070504 (2006).
53. A. Gilchrist, A. J. F. Hayes, T. C. Ralph, *Phys. Rev. A* **75**, 052328 (2007).
54. K. Kieling, T. Rudolph, J. Eisert, arXiv:quant-ph/0611140 (2006).

55. I am indebted to all my collaborators past and present who have helped in my understanding of this subject. Optical quantum computing research at Bristol is supported by the U.K. Engineering and Physical Sciences Research Council, the U.K. Quantum Information Processing Interdisciplinary Collaboration, the U.S. Disruptive Technologies Office, the E.U. Integrated Project Qubit Applications, the Leverhulme Trust, and the Daiwa Anglo-Japanese Foundation.

10.1126/science.1142892