Shor's Quantum Factoring Algorithm on a Photonic Chip

Alberto Politi,* Jonathan C. F. Matthews,* Jeremy L. O'Brien†

The realization of a quantum computer presents an exciting prospect of modern science. The processing of information encoded in quantum systems admitting quantum superposition and entanglement enables exponentially greater power for particular tasks. Originally conceived in the context of simulating complex quantum systems, it was the development of Shor's quantum factoring algorithm (*1*) that showed the capability of factoring the product of two large prime numbers exponentially faster than any known conventional method (*2*), which has ignited efforts to fabricate such a device.

Despite progress toward this goal, proof-of-principle demonstrations of Shor's algorithm have so far only been possible with liquid-state nuclear magnetic resonance (*3*) and bulk optical implementations of simplified logic gates (*4*, *5*), owing to the need for several logic gates operating on several qubits, even for small-scale compiled versions. However, these approaches cannot be scaled to a large number of qubits because of purity, size, and stability limitations of these systems. We demonstrate a compiled version of Shor's algorithm operating on four qubits in which the processing occurs in a photonic circuit of several one- and two-qubit gates fabricated from integrated optical waveguides on a silica-on-silicon chip (*6*, *7*). Whereas the full Shor's algorithm is designed to factorize any given input, a compiled version is designed to find the prime factors of a specific input.

The quantum circuit our device implements is the compiled version of Shor's algorithm for factorizing 15 (*3*–*5*) (Fig. 1A). This algorithm uses five qubits, one of which, x_0, is effectively redundant because it remains in a separable state throughout. The physical implementation (Fig. 1B) consists of two nondeterministic controlled-phase (*CZ*) gates (each with success $P = 1/9$, conditional on post selection) and six one-qubit Hadamard (*H*) gates (*8*). The computation proceeds as follows (Fig. 1, A and B): Four photons are input into the "0" or "1" waveguides to prepare the initial state $|\psi_{in}\rangle = |0\rangle_{x_1}|0\rangle_{x_2}|0\rangle_{f_1}|1\rangle_{f_2}$ (this does not represent 15 but rather the initialization for the compiled algorithm to compute the factors of 15). The *H* gates, implemented by 1/2 reflectivity directional couplers, then prepare each qubit in a superposition of 0 and 1, such that the entire state is a superposition of all possible four-bit inputs—part of the massive parallelism that gives rise to quantum speed-up. The core process is then performed by two independent *CZ* gates, each implemented by a network of three 1/3 directional couplers, that create a highly entangled output state (*4*, *5*). Measurement of the output state of qubits x_1 and x_2 and classical processing give the results of the computation (*9*).

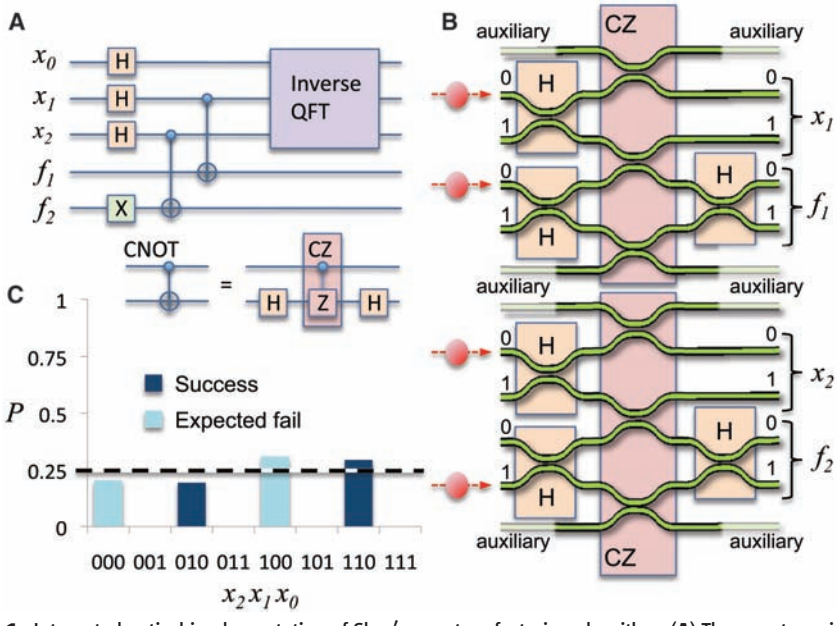

Fig. 1. Integrated optical implementation of Shor's quantum factoring algorithm. (**A**) The quantum circuit. QFT indicates quantum Fourier transform (*9*); CNOT, two qubit controlled NOT. (**B**) Schematic of the waveguide on chip device that implements the quantum computation. The x_n qubits carry the result of the algorithm; f_n are additional qubits required for the computation to work. (**C**) Outcomes of the algorithm.

We simultaneously prepared four 790-nm photons via parametric down conversion, coupled them into and out of the chip with butt-coupled arrays of optical fibers, and detected them with silicon avalanche photo diodes at a typical coincidental rate of 100 Hz per measurement (integrated for 30 s). We input the state $|\psi_{in}\rangle$ and measured the output state of qubits x_1 and x_2; the output statistics (Fig. 1C) show the four binary outcomes: 000, 010, 100, and 110 (including the x_0 qubit). Outputs 010 and 110 lead to the correct calculation for finding the order $r = 4$ for the algorithm (*9*), which then enables efficient classical computation of the factors 3 and 5; 100 gives the trivial factors (1 and 15); and 000 is an expected failure mode inherent to Shor's algorithm. The measured results have a fidelity of 99 ± 1% with the ideal probability distribution (dashed line).

This demonstration of a small-scale compiled Shor's algorithm on a chip shows promise for quantum computing in integrated waveguides. Although it currently uses an inefficient single photon source and modest efficiency detectors, ongoing progress to address heralded gates and efficient sources and detectors (*8*) combined with the results presented here will allow large-scale quantum circuits on many qubits to be implemented. Any quantum computer is a many-particle, many-path interferometer; the capability to implement such complex interferometers in a stable and miniaturized architecture is therefore critical to the future realization of large-scale quantum algorithms.

References and Notes

1. P. W. Shor, in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science* (IEEE Computer Society Press, Los Alamitos, CA, 1994), pp. 124–134.
2. This task lies at the heart of cryptographic security.
3. L. M. K. Vandersypen *et al.*, *Nature* **414**, 883 (2001).
4. C.-Y. Lu, D. E. Browne, T. Yang, J. W. Pan, *Phys. Rev. Lett.* **99**, 250504 (2007).
5. B. P. Lanyon *et al.*, *Phys. Rev. Lett.* **99**, 250505 (2007).
6. A. Politi, M. J. Cryan, J. G. Rarity, S. Yu, J. L. O'Brien, *Science* **320**, 646 (2008); published online 25 March 2008 (10.1126/science.1155441).
7. J. C. F. Matthews, A. Politi, A. Stefanov, J. L. O'Brien, *Nat. Photon.* **3**, 346 (2009).
8. J. L. O'Brien, *Science* **318**, 1567 (2007).
9. Materials and methods are available as supporting material on *Science* Online.
10. We thank R. Jozsa, A. Laing, A. Montanaro, S. Takeuchi, M. G. Thompson, and X.-Q. Zhou for helpful discussions. This work was supported by Engineering and Physical Sciences Research Council, Quantum Information Processing Interdisciplinary Research Collaboration, Intelligence Advanced Research Projects Activity, and the Leverhulme Trust. J.L.O'B. acknowledges a Royal Society Wolfson Merit Award.

Supporting Online Material

www.sciencemag.org/cgi/content/full/325/5945/1221/DC1
Materials and Methods
Fig. S1

18 March 2009; accepted 1 July 2009
10.1126/science.1173731

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.

*These authors contributed equally to this work.
†To whom correspondence should be addressed. E-mail: Jeremy.OBrien@bristol.ac.uk