Experimental Demonstration of a Compiled Version of Shor's Algorithm with Quantum Entanglement

B. P. Lanyon,[1] T. J. Weinhold,[1] N. K. Langford,[1] M. Barbieri,[1] D. F. V. James,[2] A. Gilchrist,[1] and A. G. White[1]
[1]*Department of Physics and Centre for Quantum Computer Technology, University of Queensland, Brisbane QLD 4072, Australia*
[2]*Department of Physics and Center for Quantum Information and Quantum Control, University of Toronto, Toronto ON M5S1A7, Canada*

(Received 18 May 2007; published 19 December 2007)

Shor's powerful quantum algorithm for factoring represents a major challenge in quantum computation. Here, we implement a compiled version in a photonic system. For the first time, we demonstrate the core processes, coherent control, and resultant entangled states required in a full-scale implementation. These are necessary steps on the path towards scalable quantum computing. Our results highlight that the algorithm performance is not the same as that of the underlying quantum circuit and stress the importance of developing techniques for characterizing quantum algorithms.

DOI: 10.1103/PhysRevLett.99.250505 PACS numbers: 03.67.Lx, 03.67.−a, 03.67.Mn, 42.50.Dv

As computing technology rapidly approaches the nanoscale, fundamental quantum effects threaten to introduce an inherent and unavoidable source of noise. An alternative approach embraces quantum effects for computation. Algorithms based on quantum mechanics allow tasks impossible with current computers, notably an exponential speedup in solving problems such as factoring [1]. Many current cryptographic protocols rely on the computational difficulty of finding the prime factors of a large number: a small increase in the size of the number leads to an exponential increase in computational resources. Shor's quantum algorithm for factoring composite numbers faces no such limitation, and its realization represents a major challenge in quantum computation.

To date, there have been demonstrations of entangling quantum-logic gates in a range of physical architectures, ranging from trapped ions [2,3], to superconducting circuits [4], to single photons [5–12]. Photon polarization experiences essentially zero decoherence in free space; uniquely, photonic gates have been fully characterized [6], produced the highest entanglement [8], and are the fastest of any architecture [11]. The combination of long decoherence time and fast gate speeds make photonic architectures a promising approach for quantum computation, where large numbers of gates will need to be executed within the coherence time of the qubits.

Shor's algorithm can factor a k-bit number using $72k^3$ elementary quantum gates; e.g., factoring the smallest meaningful number, 15, requires 4608 gates operating on 21 qubits [13]. Recognizing this is well beyond the reach of current technology, Ref. [13] introduced a compiling technique which exploits properties of the number to be factored, allowing exploration of Shor's algorithm with a vastly reduced number of resources. Although the implementation of these compiled algorithms does not directly imply scalability, it does allow the characterization of core processes required in a full-scale implementation of Shor's algorithm. Demonstration of these processes is a necessary step on the path towards scalable quantum computing. These processes include the ability to generate entanglement between qubits by coherent application of a series of quantum gates. In the only demonstration to date, a compiled set of gate operations were implemented in a liquid NMR architecture [14]. However, since the qubits are at all times in a highly mixed state [15], and the dynamics can be fully modeled classically [16], neither the entanglement nor the coherent control at the core of Shor's algorithm can be implemented or verified.

Here, we implement a compiled version of Shor's algorithm, using photonic quantum-logic gates to realize the necessary processes, and verify the resulting entanglement via quantum state and process tomography [17,18]. We use a linear-optical architecture where the required nonlinearity is induced by measurement; current experiments are not scalable, but there are clear paths to a fully scalable quantum architecture [19,20]. Our gates do not require preexisting entanglement, and we encode our qubits into the polarization of up to four photons. Our results highlight that the performance of a quantum algorithm is not the same as performance of the underlying quantum circuit and stress the importance of developing techniques for characterizing quantum algorithms.

Only one step of Shor's algorithm to find the factors of a number N requires a quantum routine. Given a randomly chosen co-prime C (where $1 < C < N$ and the greatest common divisor of C and N is 1), the quantum routine finds the *order* of C modulo N, defined to be the minimum integer r that satisfies $C^r \bmod N = 1$. It is straightforward to find the factors from the order. Consider $N = 15$: if we choose $C = 2$, the quantum routine finds $r = 4$, and the prime factors are given by the nontrivial greatest common divisor of $C^r/2 \pm 1$ and N, i.e., 3 and 5; similarly, if we choose the next possible co-prime, $C = 4$, we find the order $r = 2$, yielding the same factors.

Figure 1(a) shows a conceptual circuit of the quantum order-finding routine. It consists of three distinct

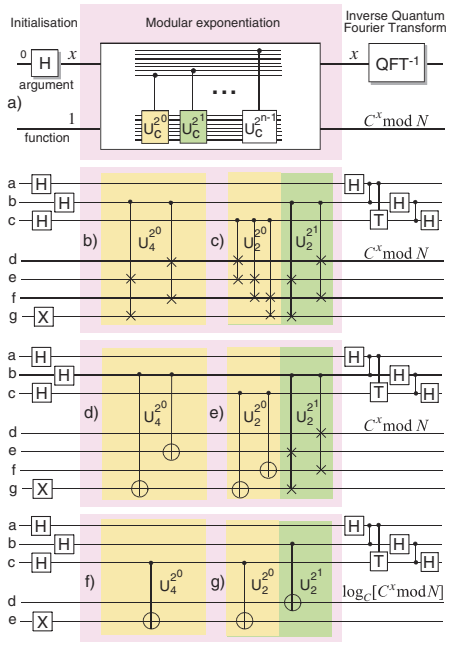

FIG. 1 (color online). (a) Conceptual circuit for the order-finding routine of Shor's algorithm for number N and co-prime C [13]. The argument and function registers are bundles of n and m qubits; the nested order-finding structure uses $U|y\rangle = |Cy \bmod N\rangle$, where the initial function-register state is $|y\rangle = 1$. The algorithm is completed by logical measurement of the argument register, and reversing the order of the argument qubits. (b,c) Implementation of (a) for $N = 15$ and $C = 4$, 2, respectively; the unitaries are decomposed into controlled-swap gates (CSWAP), marked as X; controlled-phase gates are marked by dots; H and T represent Hadamard and $\pi/8$ gates. Many gates are redundant, e.g., the second gate in (b), the first and second gates in (c). (d,e) Partially-compiled circuits of (b,c), replacing CSWAP by controlled-not gates. n.b. (e) is equivalent to the $N = 15$ $C = 7$ circuit in Ref. [14]. (f,g) Fully-compiled circuits of (d,e), by evaluating $\log_C[C^x \bmod N]$ in the function-register.

steps: (i) *register initialization*, $|0\rangle^{\otimes n}|0\rangle^{\otimes m} \rightarrow (|0\rangle + |1\rangle)^{\otimes n}|0\rangle^{\otimes m-1}|1\rangle = \sum_{x=0}^{2^n-1}|x\rangle|0\rangle^{\otimes m-1}|1\rangle$, where the argument-register is prepared in an equal coherent superposition of all possible arguments (normalization omitted by convention); (ii) *modular exponentiation*, which by controlled application of the order-finding function produces the entangled state $\sum_{x=0}^{2^n-1}|x\rangle|C^x \bmod N\rangle$; (iii) the *inverse Quantum Fourier Transform* (QFT) followed by measurement of the argument-register in the logical basis, which with high probability extracts the order r after further classical processing. If the routine is standalone, the inverse QFT can be performed using an approach based on local measurement and feedforward [21]. Note that the inverse QFT in [14] was unnecessary: it is straightforward to show this is true for any order-2^l circuit [22].

Modular exponentiation is the most computationally intensive part of the algorithm [13]. It can be realized by a cascade of controlled unitary operations, U, as shown in the nested inset of Fig. 1(a). It is clear that the registers become highly entangled with each other: since U is a function of C and N, the entangling operation is unique to each problem. Here, we choose to factor 15 with the first two co-primes, $C = 2$ and $C = 4$. In these cases, entire sets of gates are redundant: specifically, $U^{2^n} = I$ when $n > 0$ for $C = 4$, and $U^{2^n} = I$ when $n > 1$ for $C = 2$. Figures 1(b) and 1(c) show the remaining gates for $C = 4$ and $C = 2$, respectively, after decomposition of the unitaries into controlled-swap gates—this level of compiling is equivalent to that introduced in Ref. [14]. Further compilation can always be made since the initial state of the function-register is fixed, allowing the CSWAP gates to be replaced by controlled-not (CNOT) gates as shown in Figs. 1(d) and 1(e) [23].

We implement the order-2-finding circuit, Fig. 1(d). The qubits are realized with simultaneous forward and backward production of photon pairs from parametric down-conversion, Fig. 2(a): the logical states are encoded into the vertical and horizontal polarizations. This circuit requires implementing a recently proposed three-qubit quantum-logic gate, Fig. 2(b), which realizes a cascade of n controlled-z gates with exponentially greater success than chaining n individual gates [24]. The controlled-not gates are realized by combining Hadamards and controlled-z (cz) gates based on partially polarizing beam splitters. The gates are nondeterministic; when fully pre-biased, success probability is 1/4 [8–10]. A run of each routine is flagged by a fourfold event, where a single photon arrives at each output. Dependent photons from the forward pass interfere nonclassically at the first partial polarizer, Fig. 2(d); one photon then interferes with an independent photon from the backward pass at the second partial polarizer. We measure relative nonclassical visibilities, $V_r \equiv V_{\text{meas}}/V_{\text{ideal}}$, of 98 ± 2% and 85 ± 6%.

Directly encoding the order-4 finding circuit, Fig. 1(e), requires six photons and at least one three-qubit and five

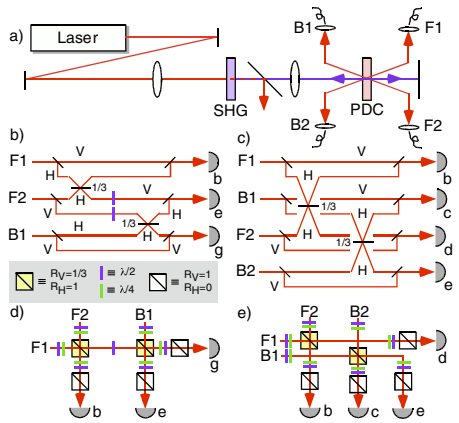

FIG. 2 (color online). Experimental schematic. (a) Forward (F1, F2) and backward (B1,B2) photons pairs are produced via parametric down-conversion [22]. (b,c) Linear-optical circuits for order-2 and order-4 finding algorithms, with inputs from (a) labeled; the letters on the detectors refer to the Fig. 1 qubits. (d,e) Physical optical circuits for (b,c), replacing the classical interferometers with partially polarizing beam splitters.

two-qubit gates. This is currently infeasible: the best six-photon rate to date [12] is 30 mHz, which would be reduced by 6 orders of magnitude using nondeterministic gates. To explore an order-4 routine, and the different processes therein, further compilation is necessary. In particular, we can compile circuits 1(d) and 1(e) by evaluating $\log_C[C^x \mathrm{mod} N]$ in the function-register in place of $C^x \mathrm{mod} N$. This requires $\log_2\{\log_C[N]\}$ function qubits, as opposed to $\log_2[N]$; i.e., for $N = 15$, $C = 2$, the function-register reduces from 4 to 2 qubits. Note that this full compilation maintains all the features of the algorithm as originally proposed in Ref. [13]. Thus, the order-4 circuit, Fig. 1(e), reduces to a pair of CNOTS, allowing us to implement the circuit in Fig. 1(g). We use a pair of compact optical gates [8–10], Fig. 2(c) and 2(e), each operating on a dependent pair of photons, resulting in measured visibilities for both of $V_r = 98 \pm 2\%$.

Figure 3 shows the measured density matrices of the argument-register output for both algorithms, sans the redundant top-rail qubit [25]. Ideally, these are maximally-mixed states [22]: in all cases, we measure near-unity fidelities [26,27]. The output of the routines are the logical state probabilities, i.e., the diagonal elements of the matrices. Combining these with the known state of the redundant qubit, and reversing the argument qubits as required, gives the binary outputs of the algorithm which after classical processing yields the prime factors of N. In the order-2 circuits the binary outputs of the algorithm are 00 or 10: the former represents the expected failure mode of this circuit, the latter a successful determination of $r = 2$; failure and success should have equal probabilities; we measure them to be 50% to within error. Thus, half the time the algorithm yields $r = 2$, which gives the factors, 3 and 5. In the order-4 circuit, the binary outputs are 000, 010, 100, and 110: the second and fourth terms yield the order-4 result, the first is a failure mode, and the third yields trivial factors. We measure output probabilities of 25% to within error, as expected. After classical processing half the time, the algorithm finds $r = 4$, again yielding the factors 3 and 5.

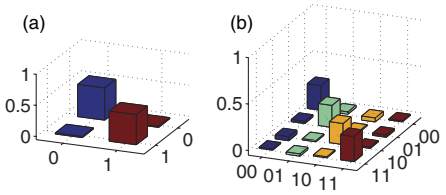

FIG. 3 (color online). Algorithm outputs given by measured argument-register density matrices. The diagonal elements are the logical output probabilities. (a) Order-2 algorithm. The fidelity with the ideal state is $F = 99.9 \pm 0.3\%$, the linear entropy is $S_L = 100 \pm 1\%$ [27]. Combined with the redundant qubit, the logical probabilities are $\{P_{00}, P_{10}\} = \{52, 48\} \pm 3\%$. (b) Order-4 algorithm, $F = 98.5 \pm 0.6\%$ and $S_L = 98.1 \pm 0.8\%$. The logical probabilities are $\{P_{000}, P_{010}, P_{100}, P_{110}\} = \{27, 23, 24, 27\} \pm 2\%$. Real parts shown, imaginary parts are less than 0.6%.

These results show that we have near-ideal algorithm performance, far better than we have any right to expect given the known errors inherent in the logic gates [8,28]. This highlights that the *algorithm* performance is not always an accurate indicator of *circuit* performance since the algorithm produces mixed states. In the absence of the gates, the argument-register qubits would remain pure; as they are mixed, they have become entangled to *something* outside the argument register. From algorithm performance, we cannot distinguish between desired mixture arising from entanglement with the function-register, and undesired mixture due to environmental decoherence. Circuit performance is crucial if it is to be incorporated as a subroutine in a larger algorithm, Fig. 1(a), 1(e), and 1(g). The *joint* state of both registers after modular exponentiation indicates circuit performance; we find entangled states that partially overlap with the expected states, Fig. 4, indicating some environmental decoherence.

Process tomography fully characterizes circuit performance, yielding the χ-matrix, a table of process measurement outcomes and the coherences between them. Measured and ideal χ-matrices can be quantitatively compared using the fidelity [6,27]; we measured process fidelities of $F_p = 85\%$, 89% for the two-qubit gates of the order-4 circuit. It is the easier of the two algorithms to characterize since it consists of two gates acting on inde-

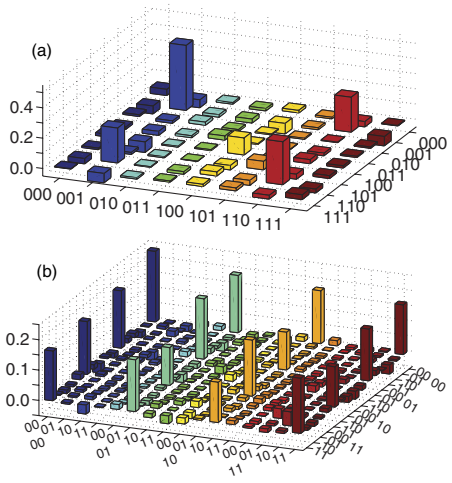

FIG. 4 (color online). Measured density matrices of the state of both registers after modular exponentiation. (a) Order-2 circuit. The ideal state is locally equivalent to a GHZ state: we find $F_{\mathrm{GHZ}} = 59 \pm 4\%$. The state is partially mixed, $S_L = 62\% \pm 4\%$, and entangled, violating the optimal GHZ entanglement witness $W_{\mathrm{GHZ}} = 1/2 - F_{\mathrm{GHZ}} = -9 \pm 4\%$ [31]. (b) Order-4 circuit. Measured fidelity with the ideal state, a tensor product of two Bell-states, is $F = 68 \pm 3\%$. The state is partially mixed, $S_L = 52 \pm 4\%$, and entangled, with tangles of the component Bell-States of $41 \pm 5\%$ and $33 \pm 5\%$. Real parts shown, imaginary parts are, respectively, less than 7% and 4%. The fidelity of the four-qubit state (b) is higher than the three-qubit state (a), chiefly because the latter requires nonclassical interference of photons from independent sources, which suffer higher distinguishability, lowering gate performance [28,32,33].

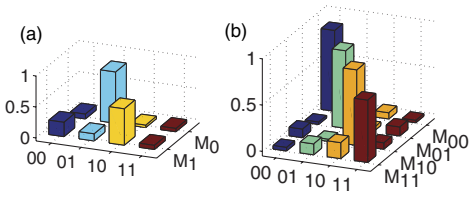

FIG. 5 (color online). Measured function-register probabilities after modular exponentiation, conditioned on logical measurement of the argument-register M_x. There is a high correlation between the registers: (a) Order-2 circuit, $\{P_{01}, P_{10}\} = \{83 \pm 4\%, 59 \pm 5\%\}$; (b) Order-4 circuit, $\{P_{00}, P_{01}, P_{10}, P_{11}\} = \{87 \pm 3\%, 84 \pm 4\%, 82 \pm 5\%, 67 \pm 6\%\}$.

pendent qubit pairs. Consequently, by assuming that only these gates induce error, the order-4 circuit process fidelity is simply the product of the individual gate fidelities [30], $F_p^{bcde} = F_p^{bd} F_p^{ce} = 80\%$. Clearly, this is significantly less than the *algorithm* success rate of 99.7%. The order-2 circuit is harder to characterize, requiring at least 4096 measurements, infeasible with our count rates. Decomposing the three-qubit gate into a pair of two-qubit gates yields process fidelities $F_p = 78\%, 90\%$ (reflecting differing interferences of independent and dependent photons). There is no simple relation between individual cz gate performances and that of the three-qubit gate. However, a bound can be obtained by chaining the gate errors, $F_p \geq 20\%$ [29]. This is not useful, c.f. the fidelity between an ideal cz and doing nothing at all of $F_p = 25\%$ (The bound only becomes practical as $F_p \to 1$). For larger circuits, full tomographic characterization becomes exponentially impractical. The order-finding routine registers contain $k = n + m$ qubits: state and process tomography of a k-qubit system require at least 2^{2k} and 2^{4k} measurements, respectively.

An alternative is to gauge circuit performance via logical correlations *between* the registers. Modular exponentiation produces the entangled state $\sum_{x=0}^{2^n-1} |x\rangle|y\rangle$ where y is respectively $C^x \mathrm{mod} N$ and $\log_C[C^x \mathrm{mod} N]$ for partial and full compilation. For a correctly functioning circuit, measuring the argument in the state x projects the function into y—requiring at most 2^k measurements to check. Figure 5 shows there is a clear correlation between the argument and function registers, 59 to 83% and 67 to 87% for the order-2 and order-4 circuits, respectively. Again, these indicative values of circuit operation are significantly less than the algorithm success rates.

We have experimentally implemented every stage of a small-scale quantum algorithm. Our experiments demonstrate the feasibility of executing complex, multiple-gate quantum circuits involving coherent multiqubit superpositions of data registers. We present two different implementations of the order-finding routine at the heart of Shor's algorithm, characterizing the algorithmic and circuit performances. Order-finding routines are a specific case of phase-estimation routines, which in turn underpin a wide variety of quantum algorithms, such as those in quantum chemistry [30]. Besides providing a proof of the use of quantum entanglement for arithmetic calculations, this work points to a number of interesting avenues for future research—in particular, the advantages of tailoring algorithm design to specific physical architectures, and the urgent need for efficient diagnostic methods of large quantum information circuits.

We wish to thank M. P. de Almeida and E. DeBenedictis for stimulating discussions. This work was supported by the Australian Research Council, Federation Fellow and DEST Endeavour Europe programs, the IARPA-funded U.S. Army Research Office Contract No. W911NF-05-0397, and the Canadian NSERC.

Note added in proof.—By better spectral filtering, we improved the GHZ state to $F = 67 \pm 3\%$, $S_L = 58 \pm 3\%$, and $W_{GHZ} = -17 \pm 3\%$.

[1] P. Shor, *Proc. 35th Ann. Symp. Found. Comp. Sci.* (IEEE Comp. Soc. Press, Los Alamitos, California, 1994), p. 124.
[2] F. Schmidt-Kaler *et al.*, Nature (London) **422**, 408 (2003).
[3] D. Leibfried *et al.*, Nature (London) **422**, 412 (2003).
[4] M. Steffen *et al.*, Science **313**, 1423 (2006).
[5] J. L. O'Brien *et al.*, Nature (London) **426**, 264 (2003).
[6] J. L. O'Brien *et al.*, Phys. Rev. Lett. **93**, 080502 (2004).
[7] P. Walther *et al.*, Nature (London) **434**, 169 (2005).
[8] N. K. Langford *et al.*, Phys. Rev. Lett. **95**, 210504 (2005).
[9] N. Kiesel *et al.*, Phys. Rev. Lett. **95**, 210505 (2005).
[10] R. Okamoto *et al.*, Phys. Rev. Lett. **95**, 210506 (2005).
[11] R. Prevedel *et al.*, Nature (London) **445**, 65 (2007).
[12] C.-Y. Lu *et al.*, Nature Phys. **3**, 91 (2007).
[13] D. Beckman *et al.*, Phys. Rev. A **54**, 1034 (1996).
[14] L. M. K. Vandersypen *et al.*, Nature (London) **414**, 883 (2001).
[15] S. L. Braunstein *et al.*, Phys. Rev. Lett. **83**, 1054 (1999).
[16] N. C. Menicucci *et al.*, Phys. Rev. Lett. **88**, 167901 (2002).
[17] D. F. V. James *et al.*, Phys. Rev. A **64**, 052312 (2001).
[18] J. F. Poyatos *et al.*, Phys. Rev. Lett. **78**, 390 (1997).
[19] E. Knill *et al.*, Nature (London) **409**, 46 (2001).
[20] M. A. Nielsen, Phys. Rev. Lett. **93**, 040503 (2004).
[21] R. B. Griffiths *et al.*, Phys. Rev. Lett. **76**, 3228 (1996).
[22] See EPAPS Document No. E-PRLTAO-99-020750 for supplementary information. For more information on EPAPS, see http://www.aip.org/pubservs/epaps.html.
[23] Figure 1(e) is equivalent to the order-4 $C = 7$ circuit in Ref. [14]: CSWAP is equivalent to a Toffoli and CNOTS.
[24] T. C. Ralph, Phys. Rev. A **70**, 012312 (2004).
[25] We use convex optimization tomography [M. De Burgh, A. Doherty, and A. Gilchrist (to be published)] and estimate errors via Monte Carlo simulation [6].
[26] Fidelity is $F(\rho, \sigma) \equiv \mathrm{Tr}[\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}]^2$; linear entropy is $S_L \equiv d(1 - \mathrm{Tr}[\rho^2])/(d-1)$, where d is the state dimension [27].
[27] A. G. White *et al.*, J. Opt. Soc. Am. B **24**, 172 (2007).
[28] T. J. Weinhold *et al.* (to be published).
[29] A. Gilchrist *et al.*, Phys. Rev. A **71**, 062310 (2005).
[30] A. Aspuru-Guzik *et al.*, Science **309**, 1704 (2005).
[31] M. Bourennane *et al.*, Phys. Rev. Lett. **92**, 087902 (2004).
[32] J. G. Rarity *et al.*, J. Opt. B **7**, S171 (2005).
[33] R. Kaltenbaek *et al.*, Phys. Rev. Lett. **96**, 240502 (2006).