Experimental Realisation of Shor's Quantum Factoring Algorithm using Qubit Recycling

E. Martín-López[1], A. Laing[1], T. Lawson[1], R. Alvarez[1], X.-Q. Zhou[1], J. L. O'Brien[1]
1. Centre for Quantum Photonics, H. H. Wills Physics Laboratory & Department of Electrical and Electronic Engineering, University of Bristol, Merchant Venturers Building, Woodland Road, Bristol, BS8 1UB, UK

Quantum algorithms are computational routines that exploit quantum mechanics to solve problems exponentially faster than the best classical algorithms. Shor's quantum factoring algorithm [1] is a key example and the prime motivator in the international effort to realise a quantum computer. However, due to the large number of resources required, to date, there have been only four small scale demonstrations [2-5]. Here we address this resource demand and demonstrate a scalable version of Shor's algorithm in which the *n* qubit control register is replaced by a single qubit that is recycled *n* times: the total number of qubits is one third of that required in the standard protocol [6]. Encoding the work register in higher-dimensional states, we implement a two-photon compiled algorithm to factor $N = 21$ [7]. Significantly, the algorithmic output exhibits structure that is distinguishable from noise, in contrast to previous demonstrations.

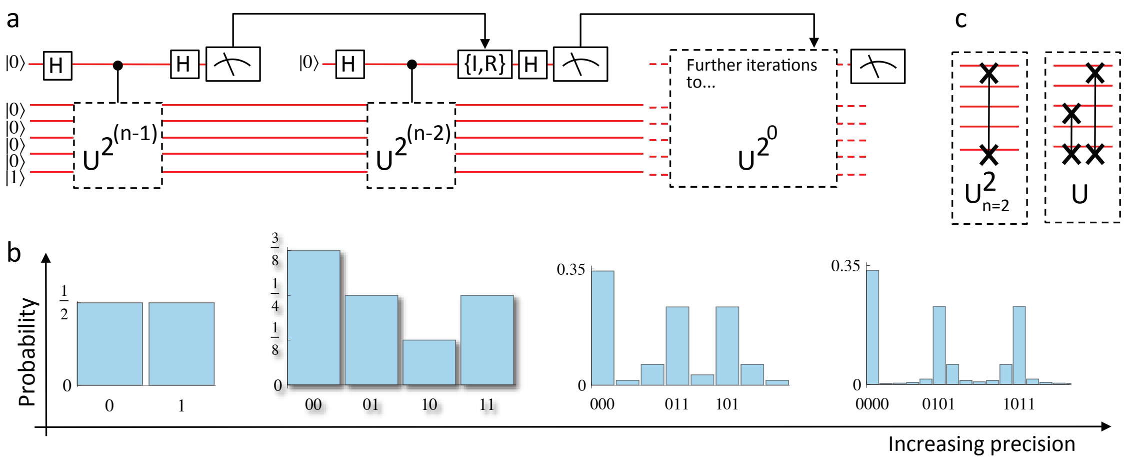

Fig. 1. **(a)** Measurement of the control qubit after each controlled unitary gives the next most significant bit in the output and the outcome is fed forward to the iterated (semi-classical) Fourier transform, which applies either the identity operation I or the appropriate phase gate R, prior to the Hadamard H. **(b)** As the number of iterations increases the precision increases. **(c)** For two bits of precision the controlled unitary operations can be constructed with this arrangement of controlled-swap gates.

The correct algorithmic output from the quantum order finding circuit for factoring $N = 21$ is confirmed by the experimental results with a fidelity of $99 \pm 4\%$ with the ideal probability distribution. The experimental output has a critical dependence on decoherence: phase instability drives the output toward a uniform probability distribution, in contrast with previous experimental demonstrations of Shor's algorithm, all of them for $N = 15$, in which a uniform probability distribution is the expected outcome. We confirmed this analysis experimentally [7].

These results point to larger-scale implementations of Shor's algorithm by harnessing substantial but scalable resource reductions applicable to all physical architectures.

References

[1] P. W. Shor in *Proc. 35th Annu. Symp. Foundations of Computer Science*, S. Goldwasser ed. (IEE Computer Society Press, Santa Fe, NM, 1994).
[2] L. M. K Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, "Experimental realization of Shors quantum factoring algorithm using nuclear magnetic resonance". Nature **414**, 883 (2001).
[3] C.-Y. Lu, D. E. Browne, T. Yang, and J.-W. Pan, "Demonstration of a compiled version of Shors quantum factoring algorithm using photonic qubits". Phys. Rev. Lett. **99**, 250504 (2007).
[4] B. P. Lanyon, T. J. Weinhold, N. K. Langford, M. Barbieri, D. F. V. James, A. Gilchrist, and A. G. White, "Experimental demonstration of a compiled version of Shors algorithm with quantum entanglement". Phys. Rev. Lett. **99**, 250505 (2007).
[5] A. Politi, J. C. F. Matthews, and J. L. OBrien, "Shors quantum factoring algorithm on a photonic chip". Science **325**, 1221 (2009).
[6] S. Parker and M. B. Plenio, "Efficient factorization with a single pure qubit and logN mixed qubits". Phys. Rev. Lett. **85**, 3049 (2000).
[7] E. Martín-López, A. Laing, T. Lawson, R. Alvarez, X-Q. Zhou, and J. L. OBrien, "Experimental realisation of Shor's quantum factoring algorithm using qubit recycling". Nature Photonics **6**, 773 (2012).

978-1-4799-0594-2/13/$31.00 ©2013 IEEE