A compiled version of Shor's quantum factoring algorithm on a waveguide chip

Alberto Politi, Jonathan C. F. Matthews & Jeremy L. O'Brien
Centre for Quantum Photonics, H. H. Wills Physics Laboratory & Department of Electrical and Electronic Engineering,
University of Bristol,
Bristol, UK,
Jeremy.Obrien@Bristol.ac.uk

Abstract—**Realization of a compiled version of Shor's quantum factoring algorithm is realized on a waveguide chip. Utilizing quantum and classical interference, multiple quantum gates are integrated within silica-on-silicon waveguide to realize a proof-of-principle of quantum computation within a single optical chip. This demonstration illustrates the importance of integrated optics for future quantum technology.**

Keywords-component; quantum information; algorithm; single photons; integrated waveguides

I. Introduction

Realizing computation based on quantum physics is one of the main goals for modern science and engineering. Fifteen years ago, Peter Shor proposed an algorithm [1] that would harness the unique quantum mechanical properties of superposition and entanglement to efficiently factorize a product of two large prime numbers [2]. To date, no known algorithm exists using conventional classical computation to solve this problem in time less than exponentially large in the input, making factorization intractable and forms the basis for most modern cryptographic security.

Progress towards proof-of-principle demonstration of Shor's factoring algorithm have included liquid state nuclear magnetic resonance [2] and bulk optical implementations using simplified quantum logic gates [3,4]. While the latter demonstrate the necessary use of entanglement required for improvement over classical computation, they cannot be scaled to the required large number of quantum gates and quantum bits (qubits). Instability and physical size remain as amongst the largest of limitations in complexity implementing practical quantum technology.

Recent demonstrations of using both lithographic and directly written monolithic waveguide circuits for quantum optical experiments [5,6,7,8,9] allows the use of integrated optics as an important platform for future quantum optical schemes. We report the subsequent application of waveguide quantum gates to realize a circuit implementing a compiled version of Shor's quantum algorithm to factorize 15 [10].

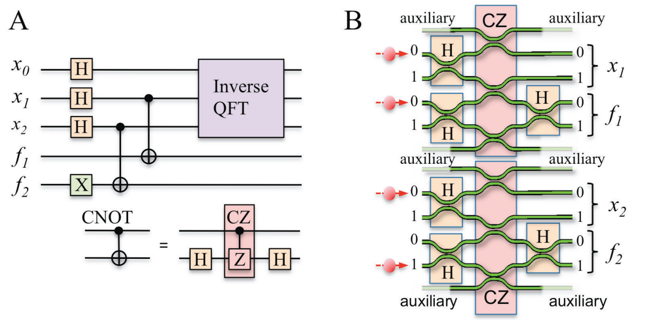

Figure 1: Realizing a compiled version of Shor's algorithm on a waveguide chip. (A) The quantum circuit compiled to factorize 15. (B) Schematic of the waveguide circuit including photonic inputs.

II. Method

The full process of Shor's algorithm can be partitioned into conventional classical processing and a quantum sub-routine known as order finding [1,3,4]. Figure 1A shows the quantum circuit for the compiled order finding routine designed specifically to factorize 15 with designed success rate of 1/2. The circuit comprises of a number of single qubit rotations (Hadamard (H), NOT (X)) and two two-qubit entangling gates (controlled π-phase shift (C-Z)) acting on qubits in two registers known as the argument (x_i) and function (f_i). An inverse quantum fourier transform (QFT) acting on the argument register is achieved for certain compiled circuits using classical post-processing [4]. The integrated waveguide version of this circuit consists of directional couplers to realize the quantum optical gates [5] and is shown schematically in figure. The 3.5μm core waveguides, designed to guide the fundamental mode for λ=790nm, are defined by doped silica on a silicon substrate and are fabricated using standard lithographic techniques [5].

Photonic quantum bits are encoded using the path of four 790nm photons simultaneously prepared via spontaneous parametric down-conversion. A 157fs Ti:sapphire laser tuned

This work was supported by Engineering and Physical Sciences Research Council, Quanutm 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.

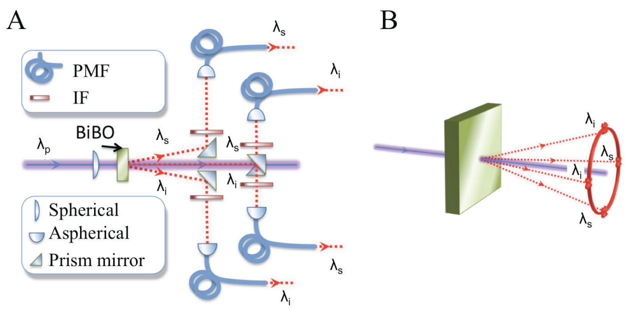

Figure 2: The down conversion based photon source. (A) Schematic of the down conversion source pumped by 390nm light to produce two pairs of 790nm photons, filtered by high transmission interference filters (IF) and collected in four spacial modes (B) into polarization maintaining fibre (PMF).

to 790nm is up-converted using a 2mm thick nonlinear bismuth borate BiB_2O_6 (BiBO) crystal (cut for second harmonic generation) to produce a beam of λ_p=385nm. This is then focused down onto a second BiBO crystal cut for spontaneous parametric down-conversion, producing pairs of signal and idler photons λ_s=λ_i=790nm, which are first filtered through high transmission interference filters (λ_0=790nm), before being collected in polarization maintaining fibres as shown in figure 2.

The photons are injected into the waveguide chip using butt-coupled arrays of polarization maintaining fibre matched to the dimensions of the waveguide circuit, and detected after the waveguide circuit using single photon counting avalanche photodiodes to yield the outcome of the quantum algorithm.

III. Results & Concluding Remarks

Detecting photons in the argument registers yields the outcome of the order finding routine. The two expected failure and two success events are predicted to occur with equal probability (1/4). Our experimental results (given in figure 3) agree with this with a similarity 99±1%. Together with final steps of classical processing, the factors of 15 are correctly determined [10].

While complete scalability of using photons to realize quantum computation is still an open area of research, needing efficient single photon sources and efficient single photon detectors, the ongoing progress in these fields together the use of ultra-stable and miniaturized integrated optical circuits, will allow the development of sophisticated quantum circuits and the implementation of large-scale quantum algorithms.

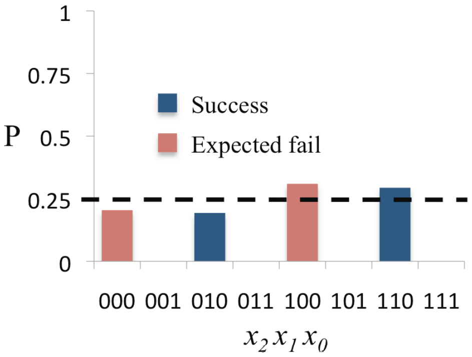

Figure 3: argument register outputs are normalized to a statistical distribution. With classical post-processing, these results reveal the factors of 15 to be 3 and 5 with success rate ½ [4,10]. The dashed line shows the ideal level of the four possible outcomes of the value, while the blue and red bars display expected success and failure outcomes of the circuit.

Acknowledgment

We thank R. Jozsa, A. Laing, A. Montanaro, S. Takeuchi, M. G. Thompson and X.-Q. Zhou for helpful discussions.

References

[1] P. W. Shor, in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science* (IEEE `Computer Science Press, Los Alamitos, CA, 1994), pp. 124-134.

[2] L. M. K. Vandersypen *et. al.*, *Nature* **414**, 883 (2001).

[3] C.-Y. Lu, D. E. Browne, T. Yang, J. W. Pan, *Phys. Rev. Lett.* **99**, 250504 (2007).

[4] B. P. Lanyon *et. al.*, *Phys. Rev. Lett.* **99**, 250505 (2007).

[5] A. Politi, M. J. Cryan, J. G. Rarity, S. Yu, and J. L. O'Brien, *Science* **320**, 646 (2008).

[6] A. Politi, J. C. F. Matthews, M. G. Thompson, J. L. O'Brien, *IEEE Journal of Selected Topics in Quantum Electronics*, **15**, 6, 1673-1684 (2009).

[7] G. D. Marshall, et al., *Optics Express*, **17**, 12546 (2009).

[8] J. C. F. Matthews, A. Politi, A. Stefanov and J. L. O'Brien, *Nature Photonics,* **3**, 346 (2009).

[9] B. J. Smith, D. Kundys, N. Thomas-Peter, P. G. R. Smith, I. A. Walmsley *Opt. Exp.* **17**, 13516 (2009).

[10] A. Politi, J. C. F. Matthews and J. L. O'Brien, *Science*, **325**, 1221 (2009).