Experimental realization of Shor's Quantum Factoring Algorithm using qubit recycling

Enrique Martín López, Anthony Laing, Thomas Lawson, Roberto Alvarez, Xiao-Qi Zhou, and Jeremy L. O'Brien

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

Motivation

Factoring large numbers is believed to be an intractable problem, requiring *exponential time*, and therefore putting large instances forever beyond the capability of conventional computers. Due to this, factoring large numbers lies at the heart of modern security protocols. In contrast, Shor's algorithm harnesses quantum-mechanical resources to address factoring in *polynomial time* [1-3].

Realizing quantum algorithms is technically challenging due to the need of many qubits and logic gates. For the first time, we address the case of factoring $N = 21$ using an iterative protocol that substantially reduces the number of qubits required in Shor's algorithm. The corresponding experimental circuit is built using linear optics.

Order Finding: The quantum core of Shor's Algorithm

To factor N following Shor's Algorithm we randomly choose a co-prime x.
To find the factors is *sufficient* to find the *order*, r, such that

$$x^r \bmod N = 1.$$

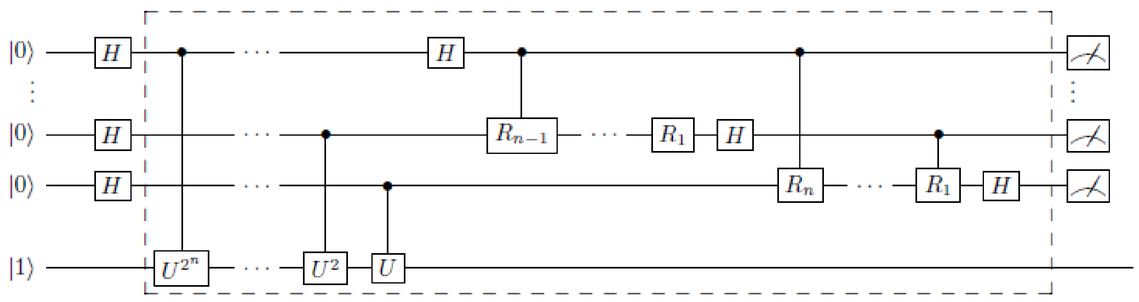
Once r is known, the factors are given by

$$\gcd(x^{r/2} \quad 1, N).$$

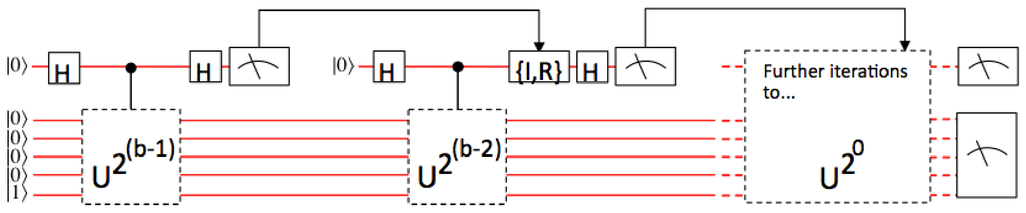
Order finding is non-tractable classically, but it is tractable using Shor's algorithm.

Input: $N = 21$ and $x = 4$ are encoded in our compiled circuit.

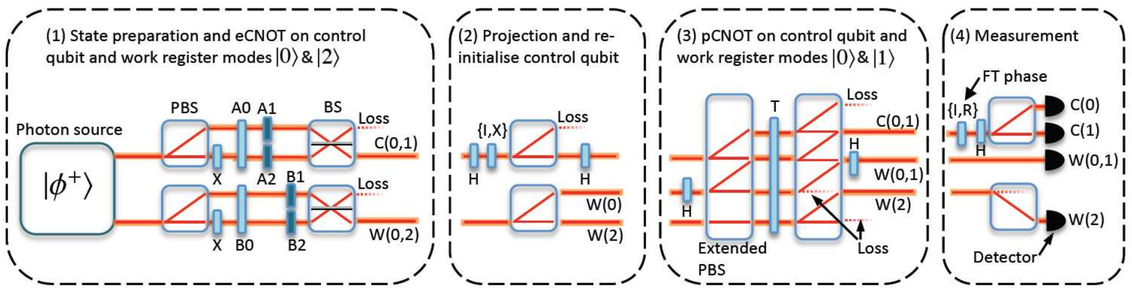
A general implementation of Shor's algorithm [4] requires many gates and qubits:



The control qubit can be recycled b times, instead of using b qubits in this register [5]:

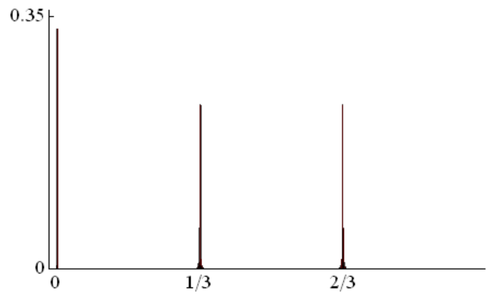


We implement two iterations in our linear optical circuit:

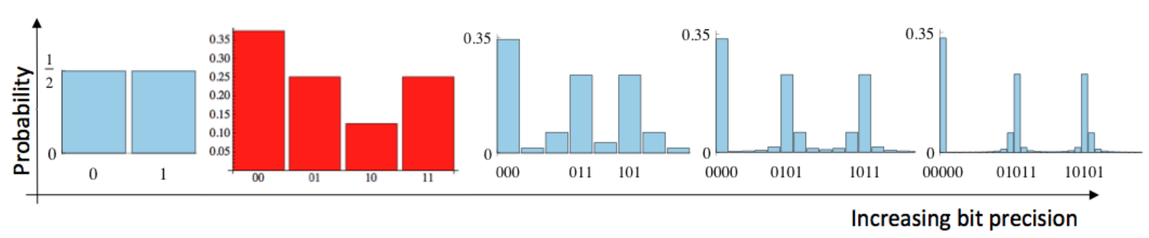


Output: Probability distribution with peaks at k/r, where $0 \le k \le r-1$

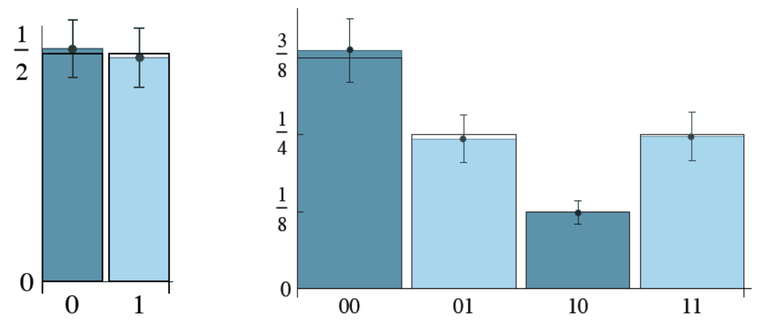
Ideal distribution for our case: $r = 3 \rightarrow 0, 1/3, 2/3$

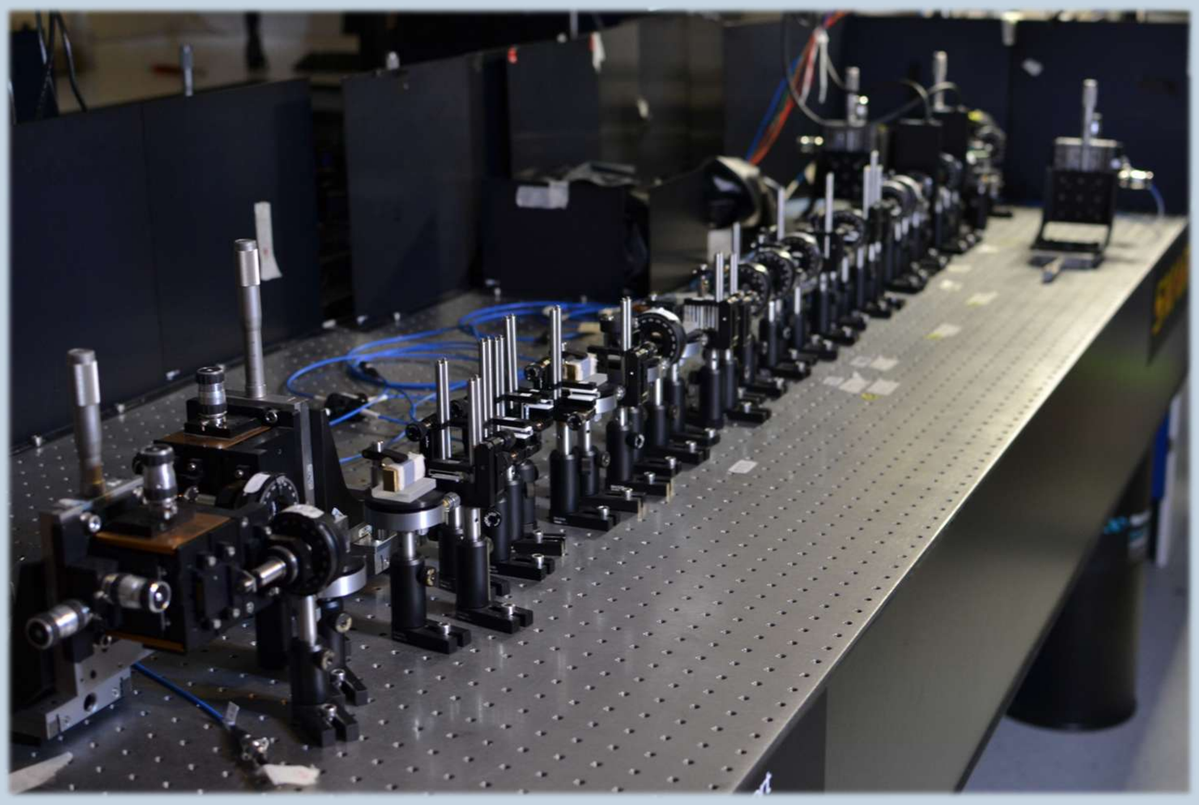


Increasing number of iterations, b, produce distributions with increasing b-bit precision:



Performing two iterations, we measure the one- and two-bit probability distributions:



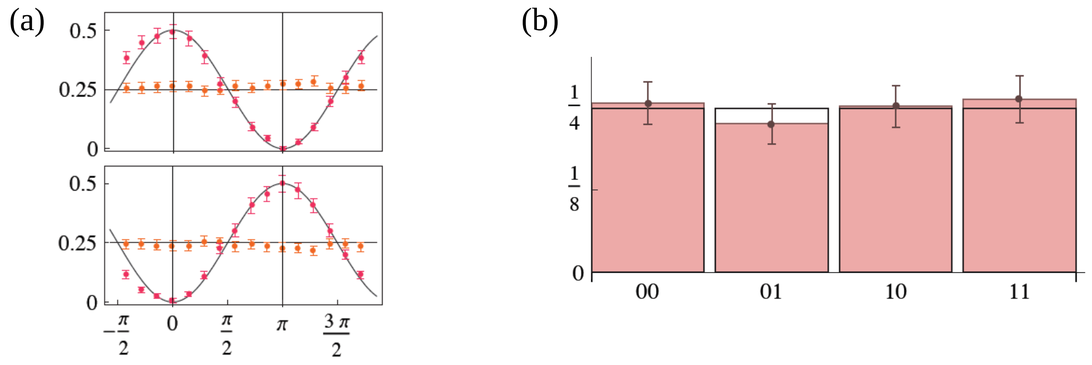


Methods and Results

Pairs of photons at 808 nm are generated using *spontaneous parametric down-conversion*. One photon of the pair encodes the control register qubit, which goes through two iterations, whereas the other photon encodes the work register in a higher dimensional *qudit* and heralds the measurement of the first photon in the control register.

We measure both the one-bit probability distribution with 99 5 % fidelity, and the two-bit probability distribution with 99 4 % fidelity, as shown in the above bar charts.

Previous experimental demonstrations of Shor's algorithm focused on $N = 15$, where there is no requirement for quantum interference in the QFT and the experimental output is consistent with noise, regardless of coprime. In contrast, $N = 21$ and coprime $x = 4$ requires genuine quantum interference in the QFT and produces a fallible experimental output in the presence of decoherence, already in the two-bit distribution:



Normalized coincidences are shown in (a) as the phase in the QFT is varied. This allows experimental simulation of decoherence in the process, which drives the probability distribution to a flat one, as shown in (b).

References

[1] R. P. Feynman, *Int. J. Thy. Phys.*, vol. 21, p. 467, 1982.
[2] D. Deutsch, Proc. R. Soc. Lond. A, vol. 400, p. 97, 1985.
[3] P. W. Shor, *Proc. 35th Annu. Symp. Foundations of Computer Science and IEEE Computer Society and Los Alamitos and CA*, pp. 124–134, 1994, ed. S. Goldwasser.
[4] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information. Cambridge University Press, 2000.
[5] S. Parker and M. B. Plenio, *Phys. Rev. Lett.* 85, 3049, 2009.