QUANTUM OPTICS

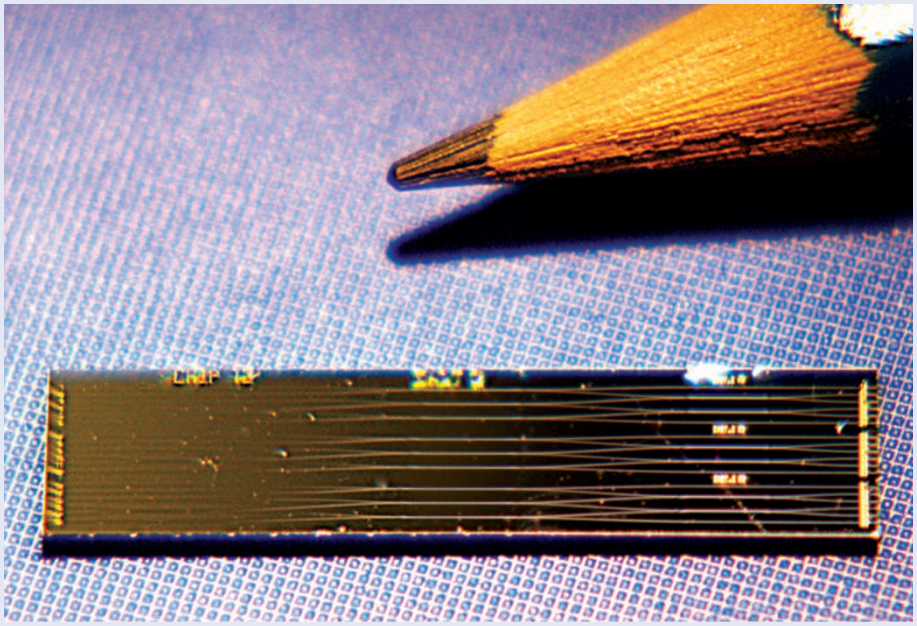
On-chip factorization

Encryption in electronic commerce is widely based on RSA — an algorithm first described by Rivest, Shamir and Adleman — which owes its security to the idea that finding factors of very large numbers is computationally impractical. In 1994, Peter Shor, a mathematics professor, presented an algorithm for a quantum computer that should be able to find factors exponentially faster than any known classical approach. In principle, this means that a sufficiently large quantum computer running Shor's algorithm could crack RSA codes.

Over the fifteen years since the original study, demonstrations of Shor's algorithm have been restricted to proof-of-principle-style quantum computer experiments based on liquid-state nuclear magnetic resonance and many optical logic gates. The drawback is that such schemes are large, complex and difficult to scale to greater computational powers — Shor's algorithm requires the use of several quantum bits (qubits), with several logic gates operating on each qubit.

Now, Alberto Politi, Jonathan Matthews and Jeremy O'Brien from the University of Bristol have reported a scalable demonstration of Shor's quantum factoring algorithm, operating on four qubits in an integrated waveguide silica-on-silicon chip (*Science* **325,** 1221; 2009).

"We implemented a compiled version of Shor's quantum factoring algorithm, which was designed to find the prime factors of 15, on a photonic chip. The chip takes four photons that carry the input for the calculation, implements Shor's algorithm, then outputs the answer — 3 and 5," O'Brien told *Nature Photonics*. "On the chip the photons travelled through silica waveguides that were brought together to form a sequence of quantum logic gates, and the output was determined by which waveguides the photons exited the chip from."



UNIVERSITY OF BRISTOL

The team used 790-nm photons generated by parametric down-conversion, butt-coupled in and out of the chip with an array of optical fibres. Detection was achieved by silicon avalanche photodiodes; that is, existing single-photon sources and detector technology. The waveguide circuit consists of a pair of two-photon entangling (controlled phase-shift) gates, and six one-qubit (Hadamard) gates. The measured results had a fidelity of 99% ± 1%, indicating unambiguous operation.

The experiment suggests that on-chip architecture is able to tackle factorization, one of the ultimate applications of quantum computing. According to O'Brien, the future challenge for the technology is to improve the performance of single-photon sources and detectors.

DAVID PILE

QUANTUM LIGHT

Sound tunes single-photon source

Controlling the transport of charge carriers between two semiconductor nanostructures using an acoustic wave yields a high-repetition-rate source of single photons with tunable emission energy.

John Cunningham

One of the most exciting challenges in quantum optics is the generation of single photons in a well-controlled manner. Sources of single photons are a fundamental requirement in quantum information processing systems, thus allowing, for example, the distribution of cryptographic keys with complete security[1]. On page 645 of this issue[2], Odilon Couto Jr and co-workers show how the controlled transfer of electrons by a surface acoustic wave (SAW) between two semiconductor nanostructures (a quantum well and quantum dot) can be exploited to generate emission of single photons (Fig. 1). The result suggests the exciting possibility of an on-demand single-photon source with tunable emission energy.