

Photon devices could outperform ordinary computers

Experiments with light confirm the need for quantum machines.

Devin Powell

21 December 2012

Advocates of 'quantum computers' say that these machines will be able to perform tasks too big for classical computers to tackle, such as cracking the codes that protect bank transactions. Now several teams have solid evidence that quantum physics does indeed embody a level of complexity that classical computers could never match. The new devices these groups have built are much simpler to build than quantum computers but could some day perform some of the same tasks.

Image courtesy of Alisha Toft

A new kind of light-manipulating device — built by researchers at the University of Queensland in Australia and elsewhere — does what no ordinary computer could ever do.

In 2010 Scott Aaronson and Alex Arkhipov, theoretical computer scientists at the Massachusetts Institute of Technology in Cambridge, wrote a long paper¹ arguing that certain quantum particles, such as photons, the quanta of light, have behaviours that are practically impossible to predict using ordinary computers. They did so by showing that the way photons interact with one another is described by mathematical rules widely believed to be 'exponentially slow' to calculate, meaning that the time it takes to get the result must increase exponentially with the number of photons.

Experimental evidence

Physicist Justin Spring at the University of Oxford and his colleagues have now proved Aaronson and Arkhipov right. In work published online in this week's *Science*, the researchers injected four identical photons into a network of beam splitters on a chip². Thanks to a quantum effect called interference — which happens when photons strike a beam splitter simultaneously — the photons take a different path through this optical maze each time the experiment is run. Detectors spot the particles at the end of each run, revealing the probabilities of arriving at all the possible destinations.

Without this device, calculating those probabilities would be mathematically difficult but not impossible; today's computers could laboriously work out the solution for four photons. But every extra particle added doubles the computational difficulty. Put 100 photons into such a device, says Aaronson, and the task outstrips the abilities of the most powerful supercomputer on the planet.

Spring's experiment could be scaled up to that size, he says, although generating the large numbers of identical photons that will require—and getting the timing just right—won't be easy. Luckily he isn't the only one with a horse in the race. A second team led by scientists at the University of Queensland in Brisbane, Australia, also unveiled its own small prototype in this week's *Science*³. And two other groups, based in Austria and Italy respectively, described similar experiments online this month in papers posted at arXiv.org^{4, 5}.

These proofs of principle have only recently become possible because laboratories are now able to produce simultaneous batches of identical photons with high reliability, Aaronson explains. The photon-based devices made so far are one-trick ponies, built purely for the sake of knowledge. "As far as we know, they have no practical use," he says. But, he adds, these photon-counting machines could some day evolve into fully operational quantum computers. "Eventually", Spring says, "we think these quantum machines could beat a classical computer."

Nature | doi:10.1038/nature.2012.12112

References

1. Aaronson, S. & Arkhipov, A. <http://eccc.hpi-web.de/report/2010/170> (2010).
2. Spring, J. B. *et al. Science* <http://dx.doi.org/10.1126/science.1231692> (2012).
3. Broome, M. *et al. Science* <http://dx.doi.org/10.1126/science.1231440> (2012).
4. Crespi, A. *et al.* <http://arXiv.org/abs/1212.2783> (2012).
5. Tillmann, M. *et al.* <http://arXiv.org/abs/1212.2240> (2012).