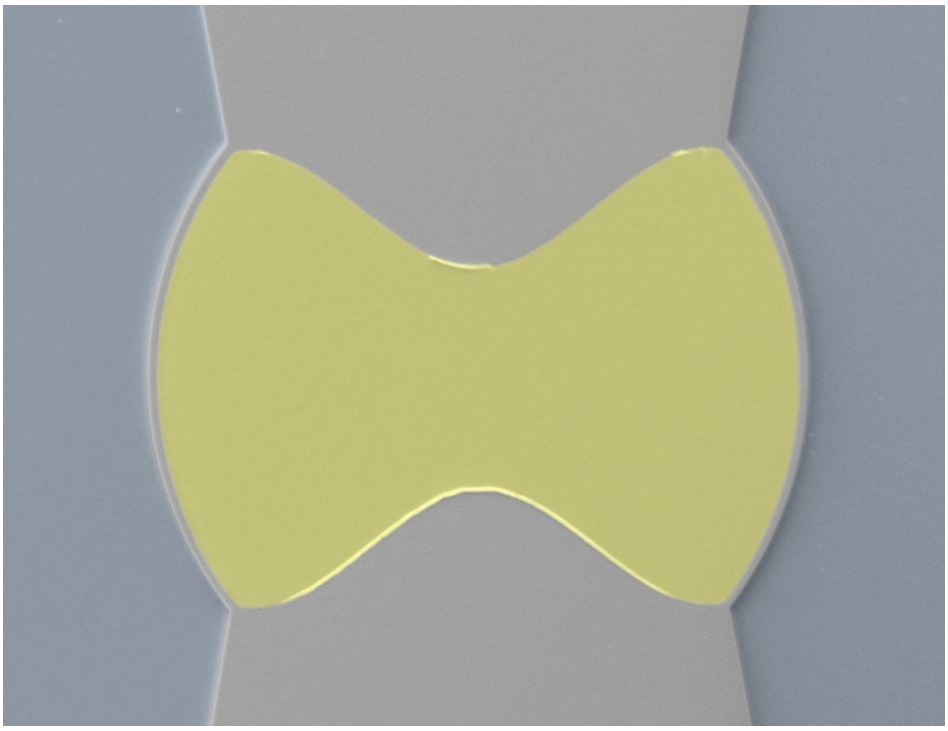
NEWS · 02 MARCH 2021

This is the fastest random-number generator ever built

Laser generates quantum randomness at a rate of 250 trillion bits per second, and could lead to devices small enough to fit on a single chip.

Davide Castelvecchi



A bow-tie-shaped semiconductor (scanning electron microscope image) produces a laser beam with randomly fluctuating intensity. Credit: Kyungduk Kim

Researchers have built the fastest random-number generator ever made, using a simple laser. It exploits fluctuations in the intensity of light to generate randomness — a coveted resource in applications such as data encryption and scientific simulations — and could lead to devices that are small enough to fit on a single computer chip.

True randomness is surprisingly difficult to come by. Algorithms in conventional computers can produce sequences of numbers that seem random at first, but over time these tend to display patterns. This makes them at least partially predictable, and therefore vulnerable to being decoded.

To make encryption safer, researchers have turned to quantum mechanics, where the laws of physics guarantee that the results of certain measurements — such as when a radioactive atom decays — are genuinely random.

A popular way to tap into quantum randomness is to exploit fluctuations in how photons are emitted by the materials used in lasers. Typical laser devices are designed to minimize these fluctuations to produce light of steady intensity: they make the light waves bounce around inside the material to force its atoms to emit more and more photons in sync with each other.

But for random-number generation, researchers aim for the opposite. “We want the intensity to fluctuate randomly, so we can

digitize the intensity to generate random numbers," says Hui Cao, an applied physicist at Yale University in New Haven, Connecticut.

Dapper device

Cao and her team made their laser material — a translucent semiconductor — in the shape of a bow tie. Photons bounce between the curved walls of the bow tie multiple times, before coming out as a scattered beam. The researchers can then capture the light with an ultrafast camera. They recorded the light output of 254 independent pixels, which together produced random bits at a rate of around 250 terabits per second, or 250 terahertz. That's several orders of magnitude faster than previous such devices, which recorded only one pixel at a time. Their results were reported in *Science* on 25 February[1].

The invention "represents a major leap in performance of random-number generators", says Krister Shalm, a physicist at the US National Institute of Standards and Technology in Boulder, Colorado.

The fastest existing computers have clock speeds measured in gigahertz, which is much too slow to fully exploit the full power of Cao's device. The set-up could be made smaller by using simpler light detectors instead of a high-speed camera. This could eventually yield practical devices small enough to fit on a single computer chip, says Cao. These could have useful applications, such as encryption technology on mobile phones.

doi: https://doi.org/10.1038/d41586-021-00562-6

References

1. Kim, K. *et al. Science* **371**, 948–952 (2021).