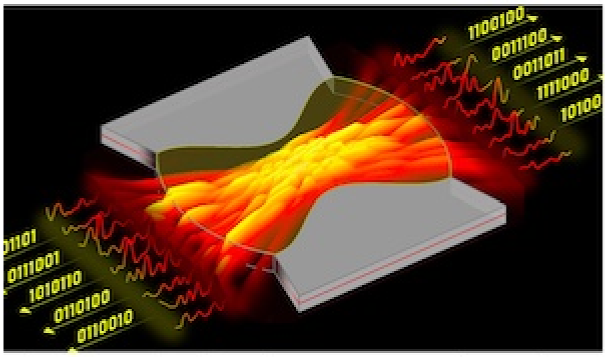
Random Numbers Faster, From a Laser

March 1, 2021 | William Weir, Yale University

Reading time 2 min (611 words)



A chip detects laser fluctuations to generate random numbers. (credit: Kyungduk Kim)

To speed things up, a team of researchers has developed a compact laser that can produce these random numbers 100 times quicker than the fastest current systems. The results are published February 26 in the journal Science.

To foil would-be hackers, computer systems need to generate sequences of random numbers. Some systems use what's known as pseudo-random numbers, which are actually complex patterns that begin with a particular number, or "seed." They work fine for some applications, but if attackers know the seed or any part of the algorithm, they can get past the encryption. Other systems employ true randomness, often relying on such unpredictable phenomena as an atom's radioactive decay, in which the timing of the decay is measured with a Geiger detector and then converted to random bits. These also have their drawbacks, such as low speed and high cost.

"Usually, those physical random number generators are not very fast — that's one problem," said Yale's Hui Cao, the John C. Malone Professor of Applied Physics and professor of physics and of electrical engineering, who led the study. "Also, they are sequential — that is, they usually just generate one bitstream. They cannot generate many bitstreams simultaneously. And in each stream, the rate is relatively low, so that prevents it from generating a lot of random numbers very quickly."

Cao and the research team designed a special type of semiconductor laser to generate randomness. The unpredictable properties of lasers have been used to generate random numbers before, but those systems relied on the lasers' chaotic temporal dynamics, which were caused by introducing feedback. However, the frequency of the fluctuations is limited by the response time of the material, which in turn limits the number of random bits those systems can produce.

Cao and her collaborators tailored their laser cavity to amplify many optical modes simultaneously. These modes will interfere with each other to generate rapid intensity fluctuations, which are recorded by a fast camera. The fluctuations at different locations are then digitized to generate many random bit streams in parallel, which translate to random numbers.

Cao compared the hourglass-shaped device to a violin which is formed specifically to amplify sound and resonate with many acoustic frequencies. Similarly, the new laser cavity acts as a resonator for optical waves and amplifies many modes of light

In all of these modes, the spontaneous emissions — caused by quantum fluctuations — make the bitstreams unpredictable, creating a massively parallel, ultrafast random bit generator. The result is a system that can generate about 250 terabits, or 250,000 gigabits, of random bits per second — more than two orders of magnitude higher than the fastest current systems. It's also energy-efficient and can be scaled up significantly.

Having demonstrated that this new physical process can be used for this purpose, Cao noted that there's still much more to study.

“It really opens a new avenue on how to generate random numbers much faster, and we have not reached the limit yet,” she said. “As to how far it can go, I think there’s still a lot more to explore.”

The researchers will next work on making the technology ready for practical use by creating a compact chip that incorporates both the laser and photodetectors. At that point, the random numbers could be fed directly into a computer.

In addition to Yale, the work is a collaboration of researchers from Université de Lorraine in France, Nanyang Technological University in Singapore, and Trinity College Dublin in Ireland. Co-authors of the study are Kyungduk Kim, Stefan Bittner, Yongquan Zeng, Stefano Guazzotti, Ortwin Hess, and Qi Jie Wang.