Pick a Number: Generating Randomness

by Chris Larson | April 2021

It might seem like the easiest problem there could be: come up with a random number. If your mind goes blank, you can throw dice, or put on a blindfold and play darts.

Shutterstock

It might seem like the easiest problem there could be: come up with a random number. If your mind goes blank, you can throw dice, or put on a blindfold and play darts. But in fact, generating random numbers is something a lot of physicists, mathematicians and computer scientists think long and hard about.

But in fact, generating random numbers is something a lot of physicists, mathematicians and computer scientists think long and hard about. They do this for a reason, or rather several reasons. Many encryption schemes for preserving the security of digital data rely on random numbers. Statistical studies are big consumers of random numbers, for simulation and other purposes; also, for some problems, algorithms that rely on randomness are more efficient or easier to implement than those that follow deterministic rules.

A study published recently in Science describes an approach to this problem using lasers. The research is the work of an international team, with Hui Cao, of the Department of Applied Physics at Yale University in New Haven, Connecticut, the corresponding author.

Random and Pseudo-Random

The study in *Science* begins by observing that modern society, so dependent on digital networks, relies crucially on "the ability to generate large quantities of randomness." The need to "improve the security of digital information has shifted the generation of random numbers from sole reliance on pseudo-random algorithms to the use of physical entropy sources." So perhaps we should begin by describing what makes something random versus pseudo-random.

A sequence of random numbers is a sequence in which you can't do better than chance in predicting the next number(s). A pseudo-random sequence, by contrast, is generated according to a definite rule, and so while it may appear to be random it is not so in fact, and if you are lucky or clever enough to learn the rule, you can predict what will come next. And in terms of cryptography, this would mean that you could decipher encrypted data.

Shutterstock/M. Bank

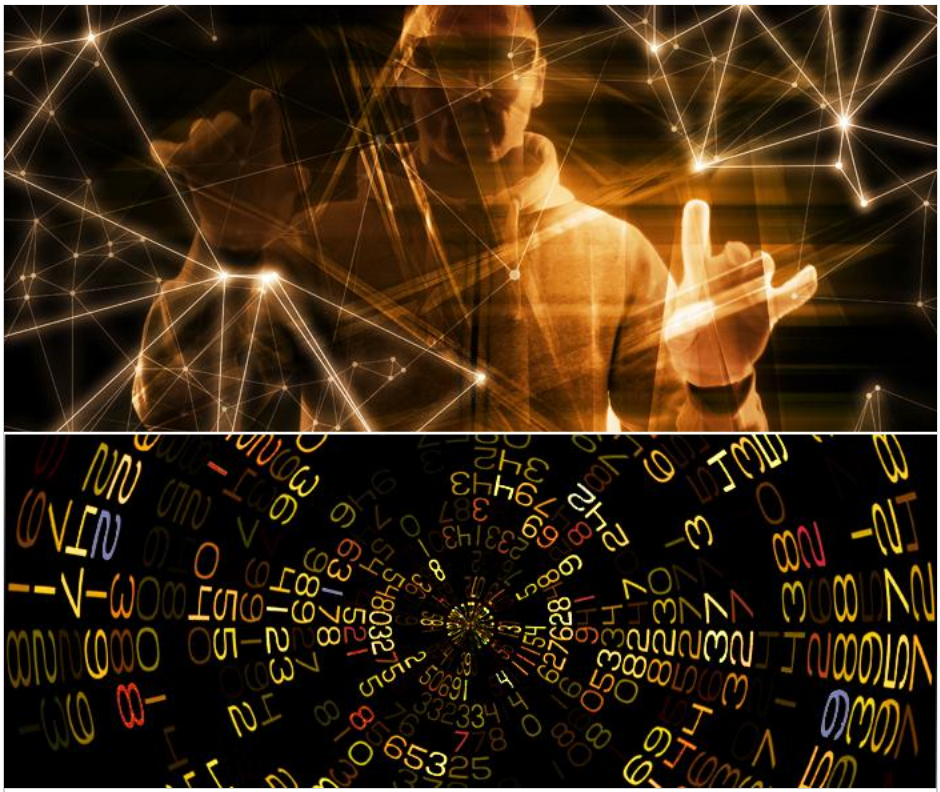
A sequence of random numbers is a sequence in which you can't do better than chance in predicting the next number(s). A pseudo-random sequence, by contrast, is generated according to a definite rule, and so while it may appear to be random it is not so in fact, and if you are lucky or clever enough to learn the rule, you can predict what will come next.

Here's an example. Consider the following sequence: 51, 37, 218, 335, 800, 2, 251…. There is no particularly obvious order to these numbers: they seem random. But in fact, they are generated by a simple mathematical formula. The formula uses modular arithmetic—that is, you do addition and multiplication and division and subtraction "modulo" a chosen number—in this case, the chosen number was 839. So, for example, 500 + 600 = 1100, but modulo 839 means "take the remainder after dividing by 839," so 500 + 600 = 1100 – (1 x 839) = 261; and, similarly, 50 x 80 = 4000, and 4000 modulo 839 is 4000 – (4 x 839) = 644. So, the formula in this case relies on picking three integers (in addition to the integer that is your modulus—in this case, 839). For this sequence, the three numbers picked were: 51, 47 and 157. The first chosen—51—is the beginning place or "seed" of the sequence. You get the second number in your sequence by operating on the first number, using a multiplication and an addition, and then reducing modulo 839. Here is how the first few numbers come:

- Second number, 37, equals 51*47 + 157, modulo 839.
- Third number, 218, equals 37*47 + 157, modulo 839
- Fourth number, 335, equals 218*47 + 157, modulo 839.

In other words, just plug in whatever you get in the nth step to the formula (n + 1 number) = (nth result) x 47 + 157, modulo 839.

This example has been explained in detail because many random number generators employed in computers and calculators in the second half of the twentieth century used only slightly more sophisticated versions of this method to generate their output. (The calculator may have shown the random number as a decimal number between 0 and 1, but the formula above can be used to provide that easily—just divide whatever number is produced by the formula by 839 and use that decimal output.)



Shutterstock/M. Bank

Algorithms may seem like an effective way of producing random numbers. But there are problems. First, given sufficient data, it is not difficult to decipher the algorithm and predict future output; and if output can be predicted, that is of course the opposite of random, and therefore, may be deciphered.

While doing the arithmetic in the example above may have seemed onerous, for a computer—even the relatively primitive computers available in 50 or 60 years ago—it is fast and easy, even if much larger numbers are used. So, algorithms such as the above may seem like an effective way of producing random numbers. But there are problems. First, given sufficient data, it is not difficult to decipher the algorithm and predict future output; and if output can be predicted, that is of course the opposite of random. And even if the algorithm is not deciphered, it is not guaranteed that the output will, in large amounts, have the characteristics of truly random output, and thus when used in simulations and statistical tests it may produce results that are not valid.

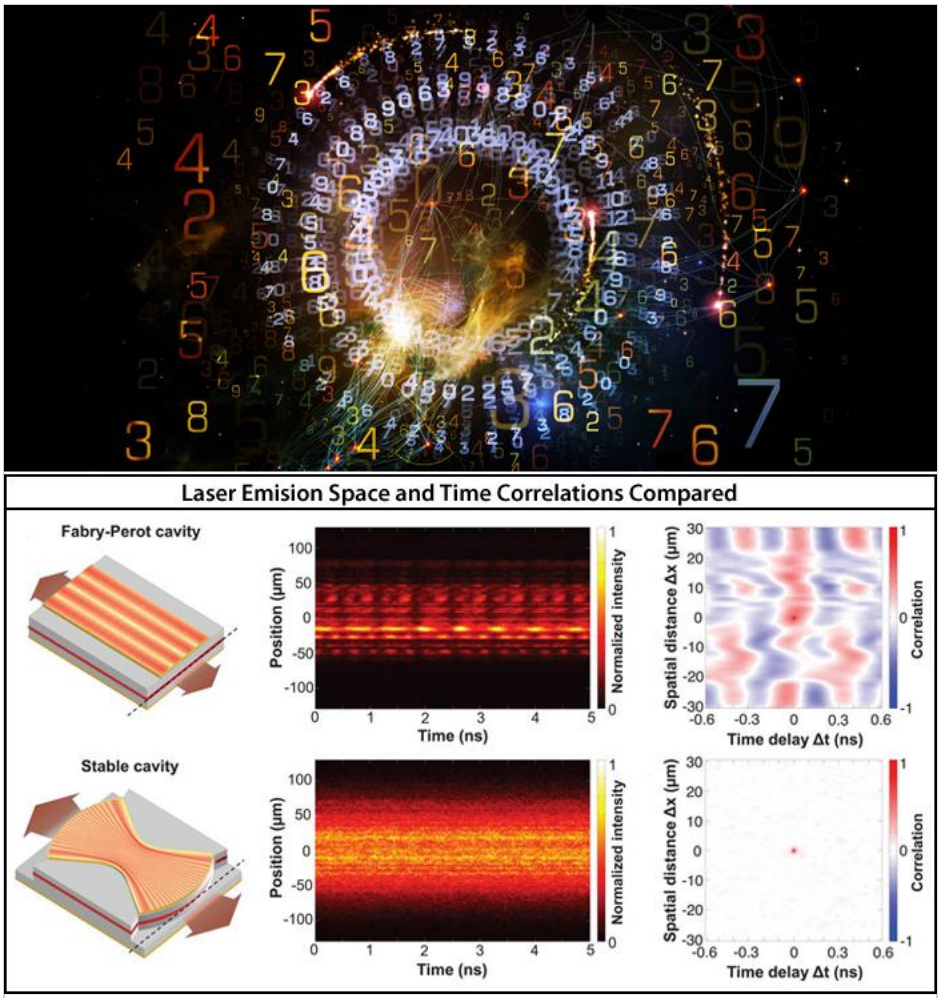
Better algorithms than the one described above can be devised that meet these objections to some extent—that is, it is more difficult to "reverse engineer" the output to decipher the algorithm, and the output may be more useful for purposes of statistical analysis. But numbers produced according to rule by an algorithm are still only "pseudo-random." Is there another approach we can use?

Nature is a huge source of randomness. Leaves fall off trees in the autumn, but we don't try to predict when an individual leaf will make the plunge—that is too random. We might have a good idea how much rain fell in a city during a two-hour rainstorm, but that knowledge doesn't translate into knowing whether the total number of raindrops in that two-hour period ended with a 0 or a 1 or 2 or some other decimal digit in the one's column—indeed, it seems pure chance. Harnessing natural processes, in other words, may be a way to access the randomness we need.

Lasers and Quantum Effects

While nature features a lot of randomness, some of it is easier to incorporate into computer technology than others. And certain parts of nature seem to be random in even more fundamental ways than others. In particular, quantum mechanics—the physics of atoms and subatomic particles—incorporates probability and randomness as an essential feature. (Albert Einstein famously expressed his reservations about this aspect of quantum mechanics, saying he was convinced that God "does not play dice with the universe." Einstein believed or hoped that quantum mechanics would eventually give way to a more complete theory that would dispense with randomness and probability; most modern physicists doubt that evolution will take place.)

At all events, the upshot is that quantum phenomena offer what would seem to be a source of true randomness. This is the background to the research by Hui Cao and her colleagues.



Top: Shutterstock; Bottom: Cao, Hue, Kyungduk Kim, et al./Science

The researchers showed how, in principle, a huge amount of random numbers could be generated. The laser can produce random bits at a rate of 250 trillion per second. The key to this was producing a broad laser with variations in intensity over the detection field, variations that were continuously changing over time, and did not betray correlations that would undercut randomness. The geometry of the laser material—the bow-tie shape—were key to achieving this.

The team used a laser to tap into this. The randomness arises “from quantum fluctuations in a laser due to a process known as spontaneous emission of photons,” according to an accompanying article in *Science* by Ingo Fischer and Daniel Gauthier, physicists working in the field but not involved in the research. Cao’s team used a translucent bow-tie shaped semiconductor as their laser material. The curved walls of the device allowed photons to bounce around and made the beam produced more scattered; this meant that the intensity of the beam would vary. Standard laser applications seek to minimize this kind of variation, but for generating randomness the opposite is desirable. Variations in intensity can be converted into a digital signal by measuring intensity at different locations and then assigning a one or zero depending on which location has the higher intensity.

Earlier research had generated random numbers using lasers along the lines indicated above, but the rate of production was low. For most applications, abundant random numbers are needed. Cao and her team showed how, in principle, a huge amount of random numbers could be generated. The laser can produce random bits at a rate of 250 trillion per second. The key to this was producing a broad laser with variations in intensity over the detection field, variations that were continuously changing over time, and did not betray correlations that would undercut randomness. The geometry of the laser material—the bow-tie shape—were key to achieving this.

The Future Is Random?

Einstein is not the only person to find randomness unappealing—for many of us, the notion of processes that are inherently chance-driven can be unsettling. But there is also something exciting about using the limitations on our knowledge—the fact that some areas of reality remain unpredictable—as a tool for expanding what we can do and learn. The many uses of random numbers do take us in that direction.

Discussion Questions

Can you think of other mathematical functions or operations that could be used to produce pseudo-random numbers?

What might be the problems, for statistical analysis, of numbers that seem to be random but in fact are not?

What other quantum phenomena besides those related to lasers might potentially by used to access randomness. Are there other areas of physics that exhibit randomness?

Journal Abstracts and Articles

(Researchers' own descriptions of their work, summary or full-text, on scientific journal websites.)

Cao, Hue, Kyungduk Kim, et al. “Massively Parallel Ultrafast Random Bit Generation with a Chip-Scale Laser.” *Science* (February 26, 2021) [accessed March 12, 2021]: https://science.sciencemag.org/content/371/6532/948?ijkey=b4ddcd29eb92749b57c6742fbbed3ecb0a183ef2&keytype2=tf_ipsecsha.

Bibliography

Cao, Hue, Kyungduk Kim, et al. “Massively Parallel Ultrafast Random Bit Generation with a Chip-Scale Laser.” *Science* (February 26, 2021) [accessed March 12, 2021]: https://science.sciencemag.org/content/371/6532/948?ijkey=b4ddcd29eb92749b57c6742fbbed3ecb0a183ef2&keytype2=tf_ipsecsha.

Castelvecchi, Davide. “This Is the Fastest Random-Number Generator Ever Built.” *Nature* (March 2, 2021) [accessed March 12, 2021]: https://www.nature.com/articles/d41586-021-00562-6.

Fischer, Ingo and Daniel J. Gauthier. “High-Speed Harvesting of Random Numbers.” *Science* (February 26, 2021) [accessed March 12, 2021]: https://science.sciencemag.org/content/371/6532/889.

Keywords

random numbers, pseudo-random numbers, modular arithmetic, modulo, encryption, cryptography, digital data, algorithms, random bit generation, lasers, Hui Cao