High-speed harvesting of random numbers

A broad-area multimode laser can be made into a powerful random number generator

By **Ingo Fischer**[1] *and* **Daniel J. Gauthier**[2]

Human-made physical random number generators (RNGs) can be traced back 5000 years or more. Early examples such as knucklebones, two-sided throwsticks, or dice have been found in the Middle East, India, and China. RNGs were used for fortune telling and games of chance, with the oldest known board games of similar age as those of the number generators. Today, RNGs are vital for services and state-of-the-art technologies such as cryptographically secured communication, blockchain technologies, and quantum key distribution. Moreover, RNGs are needed in machine learning and scientific applications such as Monte Carlo numerical methods. On page 948 of this issue, Kim *et al*. (*1*) demonstrate an ultrafast RNG based on a broad-area laser with a multispot beam that is analogous to generating random numbers by using many dice at once.

Random numbers are often generated by using a software algorithm running on a computer, called "pseudo"-random because the sequence eventually repeats. Moreover,

[1]Instituto de Física Interdisciplinar y Sistemas Complejos (IFISC), Consejo Superior de Investigaciones Científicas–Universitat de les Islas Baleares (CSIC-UIB), Campus Universitat de les Illes Balears, E-07122 Palma de Mallorca, Spain. [2]Department of Physics, Ohio State University, Columbus, OH 43210, USA. Email: ingo@ifisc.uib-csic.es; gauthier.51@osu.edu

relations among the numbers can exist that reveal that the numbers are not uniformly random. Hence, true RNGs (TRNGs) are of great interest, providing random numbers based on physical measurements that involve some noisy or stochastic process. All TRNGs have some nonidealities, such as generating zeroes more frequently than ones for a binary-output device, which must be mitigated by carefully engineering the device and postprocessing the data to improve the randomness quality (*2*).

Some applications require generating random numbers at very high rates, such as encrypting data in cloud-computing data centers, high-speed communication networks, or massive simulations. Photonic devices are a natural fit for these applications because of their potential for high-speed operation, compact size for chip-scale devices, and low power consumption.

Recently, Marangon *et al*. (*3*) developed a TRNG that is based on interfering two different lasers on a beam splitter and detecting the resulting powers that emanate from its two output ports. The randomness comes about from quantum fluctuations in a laser due to a process known as spontaneous emission of photons. This process randomizes the phase of the light emitted by each laser, and this phase variation is converted to an intensity variation through the interference effect. Measuring which output port of the interferometer has the higher or lower intensity can be used to generate a one or

a zero, respectively, at random. A compact device can be realized by generating random numbers in real time at a rate of 8 Gb/s for days at a time, passing tests that are used to assess the quality of the bit stream.

The bottleneck in reaching higher speeds is that the lasers are single-mode and only generate a Gaussian beam–like spot at a single frequency. Kim *et al*. overcome this bottleneck by using a broad-area laser that simultaneously emits a plethora of modes, resulting in a multispot beam. The patterns undergo a complex dance, writhing and growing bright and dim because of phase and amplitude variation of the light within the laser (see the figure). For a good TRNG, engineering the broad-area laser cavity is especially necessary so that spatial and temporal correlations are minimized. The authors do so, which is a major achievement.

Common broad-area lasers are known to exhibit irregular intensity pulsations in space and time because of the nonlinear interaction of light and the laser medium (*4*). Such instabilities result in correlations of their emission with characteristic spatial and temporal scales and are exceedingly difficult to avoid. This situation has plagued attempts to apply broad-area lasers more widely. Bittner *et al*. (*5*) showed that they could largely suppress the onset of spatio-temporal instabilities by using a cavity with a D shape, inspired by chaotic billiards; the balls on a D-shaped billiard table follow chaotic trajectories (*6*).

Creating bits with laser intensity

Ultrafast random bits are generated from a broad-area laser with a bow-tie cavity. In order to generate the random bits, first intensities separated by ~6 ps are subtracted from each other for the same positions on the detector. This creates bits of either ones or zeroes, which then undergo the exclusive-OR (XOR) logic operation with bits of another spot separated by half the width of the aperture. The XOR operation produces a one if the two inputs are different or a zero if the two inputs are the same. The broad-area laser allows for many different positions on the detector to be used simultaneously, allowing for fast generation of bits.
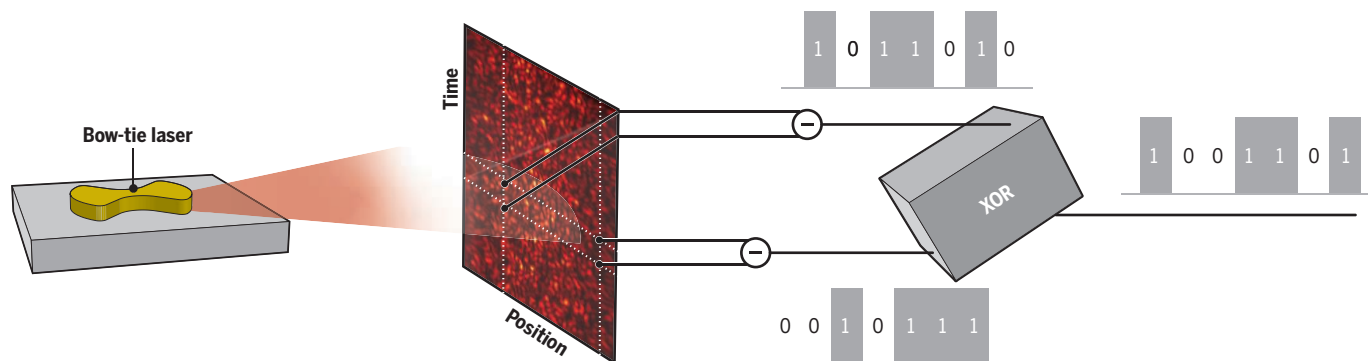
Kim *et al.* introduce another approach based on adapting the shape of the cavity. After performing extensive numerical modeling, the authors chose a bow-tie shape and precisely microfabricated a laser chip. The authors managed to boost the number of modes, avoiding their locking, and thereby substantially reduced the spatial and temporal correlation scales to 1.5 μm and 2.8 ps, respectively.

Another advantage of using the spatial degree of freedom of the special laser design is avoiding the two separate lasers and interference on an auxiliary beam splitter (*3*). Random numbers can be "harvested" from the complex emitted pattern by measuring the intensity at 254 spatial positions on ultrafast time scales (on the order of 1 ps) by using a special high-speed camera. This strategy is truly an ultrafast Demeter meeting chance.

Through this effort, they achieved a random bit generation rate of 250 Tb/s, which is much more than an order of magnitude greater than previous efforts. A full technical implementation of such an ultrafast TRNG still faces several challenges that need to be overcome. The high-speed camera could only capture data over a limited time (~2 ns), so they had to collect and concatenate multiple records to generate the more than 10^9 random numbers needed for the various statistical tests of randomness. Replacing the camera with a multitude of integrated photodetectors is yet to be achieved. Also, the required postprocessing of the measured intensities to ensure randomness is, at such speed, a task for the future.

Looking beyond, the innovative approach to tailor the spatial and temporal emission properties of broad-area lasers and manipulating the nonlinear interaction of light with the laser medium opens other applications that require many degrees of freedom. Several machine-learning approaches are based on a random mapping of low-dimensional input data onto a high-dimensional-state space, which might be accomplished by injecting a data-encoded beam into a tailored laser. Hence, broad-area lasers may become attractive photonic integrated circuits for ultrafast information processing (*7, 8*). ∎

REFERENCES AND NOTES

1. K. Kim *et al.*, *Science* **371**, 948 (2021).
2. J. D. Hart *et al.*, *Appl. Phys. Lett. Photonics* **2**, 090901 (2017).
3. D. G. Marangon *et al.*, *J. Lightwave Technol.* **36**, 3778 (2018).
4. I. Fischer, O. Hess, W. Elsäßer, E. Göbel, *Europhys. Lett.* **35**, 579 (1996).
5. S. Bittner *et al.*, *Science* **361**, 1225 (2018).
6. H. Cao, J. Wiersig, *Rev. Mod. Phys.* **87**, 61 (2015).
7. P. R. Prucnal, B. J. Shastri, *Neuromorphic Photonics* (CRC Press, 2017).
8. D. Brunner, M. C. Soriano, G. Van der Sande, Eds., *Photonic Reservoir Computing* (De Gruyter, 2019).

10.1126/science.abg5445

Optimizing age-specific vaccination

Vaccination strategies are not one-size-fits-all

By **Meagan C. Fitzpatrick**[1,2] *and* **Alison P. Galvani**[2]

E
fficacious vaccines against severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) have been developed, tested, and approved for emergency use with unprecedented speed. Deployment of multiple vaccines was initiated in several countries less than 1 year after identification of the virus. Although vaccine production is being rapidly scaled up, demand will exceed supply for the next several months. Consequently, an urgent challenge is the optimization of vaccine allocation to maximize public health benefit. On page 916 of this issue, Bubar *et al.* (*1*) demonstrate that vaccination of older people is the optimal age-based strategy to alleviate the burden of COVID-19. Although vaccination of younger adults is projected to avert the greatest incidence, vaccinating older adults will most effectively reduce mortality. In addition, they assess targeted vaccination that was based on serological status, finding that vaccinating seronegative individuals improves efficiency especially in settings where seroprevalence is high.

Some have looked to influenza vaccination strategies for guidance, given that SARS-CoV-2 is a respiratory virus with similar modes of transmission (*2*). Until 2008, the U.S. Centers for Disease Control and Prevention (CDC) prioritized people aged 50 years and older for influenza vaccination because of their increased risk of mortality (*3*). To evaluate this long-standing policy, optimal influenza vaccine allocation was determined on the basis of a dynamic transmission model combined with optimization algorithms that facilitated the searching of wide ranges of parameter space across multiple dimensions concurrently (*4*). The dynamic model component simulates both the direct protection conferred to a vaccinated individual as well as the indirect protection for others that is attributable to reductions in onward trans-

mission. This modeling indicated that allocating scarce vaccines to school-age children and young adults achieves the most effective reduction in influenza burden whether measured in terms of incidence, hospitalizations, years of life lost, or economic cost (*4*). These insights prompted an expansion of recommendations to prioritize school-age children (*5*), which interrupts transmission for all ages and bolsters indirect protection against mortality. Bubar *et al.* extend the framework of transmission modeling combined with vaccine optimization developed for influenza (*4*) to explore SARS-CoV-2 vaccination strategies and, different from the optimal influenza vaccination strategy, they conclude that vaccinating older people most effectively mitigates mortality from COVID-19.

Although it may seem intuitive that the optimal strategies against influenza and COVID-19 would be identical, vaccine optimization is not one size fits all, even for apparently similar pathogens. Quantitative changes in the epidemiological landscape can lead to qualitative shifts in optimization (see the figure). The age-specific probability of infection is a key component of this landscape. As a result of contact patterns, older people are simultaneously less exposed to and less responsible for onward transmission of both influenza virus and SARS-CoV-2 (*6*). An awareness of their heightened risk for severe clinical outcomes from COVID-19 has further suppressed contacts of older people. By contrast, essential workers, who are more likely to be exposed to SARS-CoV-2, are usually younger adults. These behavioral factors point to reduced public health benefit from vaccination of older people, but there are other factors that must also be considered.

Vaccine efficacy also affects optimization. Vaccines that elicit more efficacious direct protection against infection concomitantly generate stronger indirect effects (*7*). Highly efficacious vaccines administered to younger people can efficiently interrupt transmission chains, whereas modestly efficacious vaccines do not. With everything else being equal, vaccine efficacy as high as so far reported for SARS-CoV-2 vaccines also favors prioritization of younger people (*7, 8*). A caveat is that clinical tri-

[1]Center for Vaccine Development and Global Health, University of Maryland School of Medicine, Baltimore, MD, USA. [2]Center for Infectious Disease Modeling and Analysis, Yale School of Public Health, New Haven, CT, USA. Email: alison.galvani@yale.edu

Science

High-speed harvesting of random numbers

Ingo Fischer and Daniel J. Gauthier

ARTICLE TOOLS	http://science.sciencemag.org/content/371/6532/889
RELATED CONTENT	http://science.sciencemag.org/content/sci/371/6532/948.full
REFERENCES	This article cites 6 articles, 2 of which you can access for free http://science.sciencemag.org/content/371/6532/889#BIBL
PERMISSIONS	http://www.sciencemag.org/help/reprints-and-permissions

Use of this article is subject to the Terms of Service