CHAOTIC LASERS

The world's fastest dice

The dynamics of chaotic lasers can be harnessed to create a random-number generator that works at an astonishing rate. Such a generator could be implemented to make storage and transfer of data more secure at very high speeds.

Thomas E. Murphy* and Rajarshi Roy†
are in the Institute for Research in Electronics and Applied Physics, University of Maryland, College Park, Maryland 20742-3511, USA.
e-mail: *tem@umd.edu; †rroy@umd.edu

GETTY

Atsushi Uchida and co-workers use chaotic semiconductor lasers for fast random-number generation.

Unlike gambling, cryptography, weather prediction and economic forecasting, generating random numbers is not an ancient enterprise. But, the art and science of generating random numbers has rapidly become crucial in all of these pursuits plus many more. Consequently, producing such numbers and discerning whether they are truly random is of growing importance. On page 728 of this issue, Atsushi Uchida and co-workers introduce a novel technique for generating random numbers at unprecedented rates (1.7 Gbit s^{-1}) using chaotic dynamics in laser systems[1].

Methods for generating random numbers can be divided into either software- or physical-based approaches. Software-based random-number generators rely on numerical algorithms to produce irregular sequences of numbers that seem random and unpredictable. Numbers generated in this way are actually only pseudorandom: two systems that begin in the same initial state will produce identical sequences. For many applications, including Monte-Carlo simulation and stochastic modelling, this limitation is tolerable, and in certain cases desirable. The vast majority of today's computer telecommunications, online commerce and data encryption systems rely on such pseudorandom generators for producing the keys used to securely store and transmit data.

The advantage of software-based random-number generation is that it is inexpensive and can, in principle, operate at rates limited only by the processor speed. The disadvantage, however, is that because it is not truly random, it is vulnerable, especially if an attacker can acquire partial knowledge about the algorithm or its initial state. The famous statement by John von Neumann[2], "Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin," reminds us of the limitations of deterministic schemes for random-number generation. As an example of the pitfalls of software-based random-number generation, as recently as November 2007, researchers reported vulnerability in the pseudorandom generator that is widely used in Microsoft products to produce cryptographically secure random numbers[3].

By contrast, physical approaches to random-number generation rely on inherently random or unpredictable processes in the physical world. Such events could be either fundamentally random, as for example with quantum-mechanical uncertainty or thermal noise, or deterministic but difficult to predict phenomena, such as rolling dice[4], coin tossing[5,6] or the spin of a roulette wheel. These, and systems like them, exhibit a sensitive dependence on initial conditions.

Recent work has focused on quantum-mechanical random-number generators that generate bits based on whether or not a photon is detected[7–9]. Such systems are appealing both because the randomness is based on fundamental quantum principles, and also because the inherently discrete nature of photon counting alleviates, to some extent, the need for threshold detection of an analog variable. Although such systems are now commercially available[10], they are restricted to rates below around 20 Mbit s^{-1} because of the limited speed of photon-counting circuitry. Although gigahertz photon-counting detectors are available, such systems are expensive, often require either cooling or high voltages, and are ill-suited for compact random-number generators.

Other approaches to physical random-number generators have used the electrical noise from diodes or resistors — analog random signals that originate from thermal fluctuations that are present in any electrical system operating above absolute zero temperature. Random bits are generated by amplifying the analog signal and detecting whether or not it falls above a decision threshold. Because of the low signal level, such systems are highly susceptible to bias from small non-random external perturbations, including temperature fluctuations.

The results of Uchida *et al.* are of particular interest for two reasons. First, it reports the generation of random numbers (certified as such by several standard benchmark tests) at a significantly faster rate than any other physical system has achieved so far. Second, the researchers take the not so obvious approach of using chaotic semiconductor lasers. These devices can amplify small physical fluctuations that may have quantum-mechanical origins. Quantum fluctuations, arising from spontaneous emission of photons, provide an element of underlying randomness that is in turn amplified by chaotic dynamics to a macroscopic fluctuating signal. This signal can be readily detected using conventional photodetectors and electronics that are much faster than the photon-counting detectors required by quantum optical systems. The amplification of small fluctuations by chaotic processes is an intrinsic property of chaotic dynamical systems, and an essential component of the technique.

In a conventional laser, the emitted light, which originates from background quantum fluctuations due to spontaneous emission, settles into a steady state after repeated amplification through stimulated emission. In the semiconductor lasers used in this experiment, the orderly

stimulated emission process is plunged into a state of chaotic disorder when light re-enters the cavity after reflection from an external mirror. The lasers emit light with uncorrelated macroscopic fluctuations that occur at very high speeds. The technique uses beams of light from two lasers that fluctuate independently to generate the random numbers through an XOR (one or the other but not both) operation. This ensures that any temporal correlation of a single source is removed.

The present experiment can thus be regarded as a beautiful example of partnership between quantum fluctuations and chaotic dynamics at the macroscopic level. It illustrates how large, easily detected fluctuations can emerge from truly random quantum fluctuations, connected by the bridge of a nonlinear dynamical system — the semiconductor laser with optical feedback. The three elements of quantum fluctuations, nonlinearity and time-delayed feedback work together in this experiment to produce a virtually inexhaustible store of random numbers at the highest speeds achieved so far. This is an example of nature helping us with a difficult (according to Von Neumann, impossible) mathematical task.

References

1. Uchida, A. *et al. Nature Photon.* **2,** 728–732 (2008).
2. von Neumann, J. *J. Res. Natl Bur. Stand. Appl. Math. Ser.* **12,** 36–38 (1951); reprinted *John von Neumann Collected Works* Vol. 5 (ed. Taub, A. H.) 768–770 (New York, Macmillan, 1963).
3. Dorrendorf, L., Gutterman, Z. & Pinkas, B. in *Proc. 14th ACM Conf. Computer Commun. Security* 476–485 (2007).
4. Galton F. *Nature* **42,** 13–14 (1890).
5. Ford, J. *Phys. Today* **36,** 40–47 (1983).
6. Diaconis, P., Holmes, S. & Montgomery, R. *SIAM Review* **49,** 211–235 (2007).
7. Stefanov, A., Gisin, N., Guinnard, O., Guinnard, L. & Zbinden, H. *J. Mod. Opt.* **47,** 595–598 (2000).
8. Jennewein, T., Achleitner, U., Weihs, G., Weinfurter, H. & Zeilinger, A. *Rev. Sci. Instrum.* **71,** 1675–1680 (2000).
9. Dynes, J. F., Yuan, Z. L., Sharpe A. W. & Shields, A. J. *Appl. Phys. Lett.* **93,** 031109 (2008).
10. http://www.idquantique.com/products/quantis.htm

OPTICAL DELAY

Slower for longer

Coupled optical microresonators are one way of slowing down light. A new record has now been set for the length of these slow-light waveguides using an array of more than 100 photonic-crystal cavities.

Richard M. De La Rue

is in the Optoelectronics Research Group, Department of Electronics and Electrical Engineering, University of Glasgow, Rankine Building, Oakfield Avenue, Glasgow, G12 8LT, Scotland, UK.

e-mail: R.Delarue@elec.gla.ac.uk

A remarkably compact 'slow-light' delay line has been realized by coupling as many as 200 high-quality-factor microresonators together sequentially. The results, reported on page 741 of this issue[1] by Masaya Notomi and his co-workers at NTT's research labs in Atsugi, Japan, represent a noteworthy advance in photonic-crystal (PC) research. The device (Fig. 1) is a specific example of a coupled-resonator optical waveguide (CROW), which has been investigated by various research groups[2–5]. As measured by the large number of resonator elements used and the small size of the device footprint, the results of Notomi and co-workers are impressive. Such delay lines have interesting potential for applications in photonic-signal processing and optical memory.

Light typically propagates more slowly in solid media than in free space. The amount by which the light is slowed down is called the refractive index. At optical frequencies, the largest available refractive index in a transparent solid material is about 4. Modern optical-fibre communication systems use fine threads of highly transparent silica glass, exploiting the fact that light can be transmitted over long distances with small propagation losses, about 0.2 dB km^{-1}, and with large information bandwidths of several tens of gigabits per second. The delay on an optical signal as it passes along such a silica fibre can be thought of as a purely optical form of memory. A back-of-the-envelope calculation shows that 100 km of fibre stores, in pipe-line mode, approximately 50 Mbit of information, even if the data rate pumped through the fibre is as high as 100 Gbit s^{-1}. However, a coil that contains 100 km of fibre is not a compact object, particularly when compared with a silicon-based electronic memory that can store the same amount of information. Nor is it easy to get access to the information in a fibre

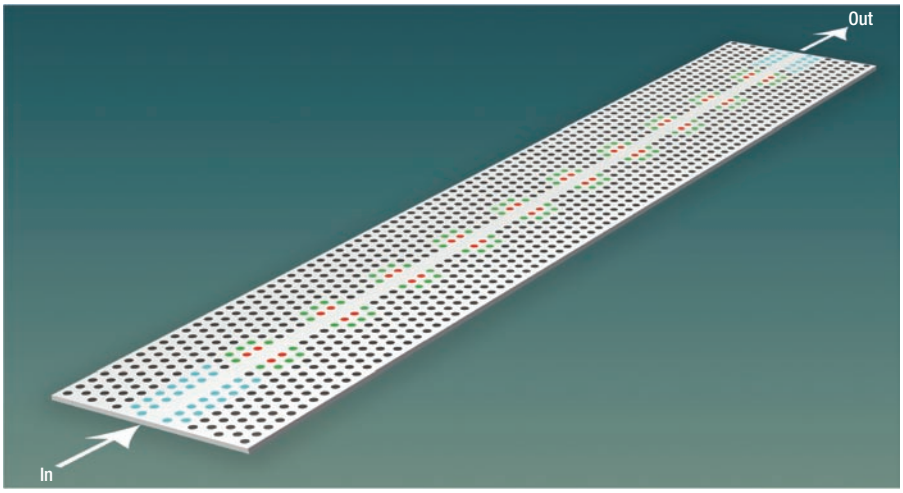

Figure 1 Schematic of a short (ten resonators) PC CROW. The design is based on a uniform PC lattice with identical sections of uniform channel guide, which link identical resonator regions formed by small, but carefully designed and fabricated, regions of deformed PC lattice.