Perfect chaos

Laser noise and chaos are unwanted elements in most circumstances. However, scientists have now learnt how to put them to good use to generate high-quality random bit sequences. Atsushi Uchida from Saitama University in Japan tells *Nature Photonics* how.

Why are random numbers important?
Randomness refers to a lack of predictability, and its generation involves a non-deterministic pattern that is non-reproducible and statistically unbiased. Random numbers are needed for information security to ensure confidentiality through encryption, authentication by challenge–response protocols and data integrity using digital signatures. The generation of random numbers is implemented when we send e-mails and make online transactions. Besides, trusted random numbers are used to select photon-detection parameters in quantum cryptography and Monte Carlo numerical simulations to solve problems in the fields of nuclear medicine, computer graphics, finance, biophysics, computational chemistry and materials science.

What is the motivation for your work?
Pseudo-random number generators, which use a single 'seed' to generate random numbers based on deterministic algorithms, have been developed and are widely used in modern digital electronic information systems. However, the generated random numbers can be predicted and reproduced if the single seed is known or guessed by invaders. Physical non-deterministic random-number generators based on entropy sources have also been developed by using random physical phenomena, such as photon noise, the thermal noise in resistors, and the frequency jitter of oscillators. However, owing to the limitations of the mechanisms of extracting bit sequences, the generation speed is much slower than pseudo-random-number generators. So far, only about 10 Mbit s^{-1} and 4 Mbit s^{-1} are achievable in single devices using electronic oscillator jitter and quantum optical noise, respectively. Achieving higher rates of up to 100 Mbit s^{-1} and above requires a combination of several such devices. To be compatible with current computation and communication systems, speeds of more than 1 Gbit s^{-1} are required. In 2002, we started experiments on the use of rapidly fluctuating signals in semiconductor lasers to generate secure keys for protecting information. That led to the idea of high-bit-rate random-number generation using physical chaos in semiconductor lasers.

ATSUSHI UCHIDA

Back row (left to right): Kazuyuki Yoshimura, Isao Oowada, Atsushi Uchida, Kazuya Amano and Peter Davis. Front row (left to right): Kunihito Hirano and Hiroyuki Someya.

What is the physical mechanism of your approach?
First, semiconductor lasers with relaxation oscillation frequencies of more than a few gigahertz are needed. Second, intrinsic laser noise that provides unpredictability of small fluctuations over wide frequency ranges is highly desired. Third, and most importantly, we exploit the chaos in lasers that causes nonlinear amplification and mixing of the laser noise, producing large amplitude oscillations that can be used to generate digital bits with robust statistical properties. The amplification of microscopic laser noise by chaotic dynamics assures the non-deterministic property of the bit sequences.

How did you achieve a high bit rate?
Our approach uses two broadband semiconductor lasers with chaotic intensity oscillations. The output intensity of each laser is converted to an a.c. electrical signal by photodetectors, then amplified and converted to a binary signal using a 1-bit analog-to-digital converter driven by a fast clock. The binary bit signals obtained from the two lasers are combined, to obtain a single random bit sequence at a high bit rate. Two lasers are needed to pass the stringent statistical tests of randomness. Bit sequences generated by a single laser exhibit subtle repetition features owing to harmonic relations between the characteristic laser oscillation components and the clock. Better-quality randomness can be generated by adjusting the control parameters of two lasers to detune the main periodic components of the chaotic oscillations. In other words, we control the delay time of the optical feedback and the periods of the largest chaotic oscillation components so that they neither match with each other nor the clock period.

What are the implications of your achievement?
We generate random bit sequences at rates of up to 1.7 Gbit s^{-1}. This rate is an order of magnitude faster than previously reported devices for physical random-bit generators with verified randomness. The scheme requires only readily available chaotic semiconductor lasers, and thus can be easily implemented. Our findings may lead to improved security, as they will enable the use of truly random numbers in public cryptography, resulting in less reliance on pseudo-random-number generators, which are vulnerable to attacks. The high rate of random-bit generation achieved may also improve the speed of secure key generation in future quantum cryptography systems.

What are your future plans?
We are looking at increasing the bandwidth of the laser chaos to increase the rate of generation, and reducing the size of the system to implement a physical random-number generator in a small module or chip. We also hope to gain a better understanding of the fundamental process of amplification of laser noise by chaotic laser dynamics.

Interview by Rachel Won.

Uchida and co-workers have a Letter on fast physical random-bit generation using chaotic semiconductor lasers on page 728 of this issue.