Fast physical random bit generation with chaotic semiconductor lasers

ATSUSHI UCHIDA[1,2]*, KAZUYA AMANO[1], MASAKI INOUE[1], KUNIHITO HIRANO[1], SUNAO NAITO[1], HIROYUKI SOMEYA[1], ISAO OOWADA[1], TAKAYUKI KURASHIGE[1], MASARU SHIKI[1], SHIGERU YOSHIMORI[1], KAZUYUKI YOSHIMURA[3] AND PETER DAVIS[3]

[1]Department of Electronics and Computer Systems, Takushoku University, 815-1 Tatemachi, Hachioji, Tokyo 193-0985, Japan
[2]Department of Information and Computer Sciences, Saitama University, 255 Shimo-Okubo, Sakura-ku, Saitama city, Saitama 338-8570, Japan
[3]NTT Communication Science Laboratories, NTT Corporation, 2-4 Hikaridai, Seika-cho, Soraku-gun, Kyoto 619-0237, Japan
*e-mail: auchida@mail.saitama-u.ac.jp

Published online: 23 November 2008; doi:10.1038/nphoton.2008.227

Random number generators in digital information systems make use of physical entropy sources such as electronic and photonic noise to add unpredictability to deterministically generated pseudo-random sequences[1,2]. However, there is a large gap between the generation rates achieved with existing physical sources and the high data rates of many computation and communication systems; this is a fundamental weakness of these systems. Here we show that good quality random bit sequences can be generated at very fast bit rates using physical chaos in semiconductor lasers. Streams of bits that pass standard statistical tests for randomness have been generated at rates of up to 1.7 Gbps by sampling the fluctuating optical output of two chaotic lasers. This rate is an order of magnitude faster than that of previously reported devices for physical random bit generators with verified randomness. This means that the performance of random number generators can be greatly improved by using chaotic laser devices as physical entropy sources.

The performance and reliability of our digital networked society relies on the ability to generate large quantities of randomness. Random numbers are commonly used in computations to solve problems in nuclear medicine, computer graphics, finance, biophysics, computational chemistry and materials science[3]. Also, random numbers are used in transactions on the internet to ensure confidentiality (encryption), authentification (challenge–response protocols) and data integrity (digital signatures)[1,2]. Future deployments of quantum cryptography systems will require the generation of trusted random numbers to select photon detection parameters[4]. Efforts are being made to develop faster and more reliable generators and establish better standards for random number generation based on stringent tests of randomness[5–7].

Truly random numbers should be unpredictable, unreproducible and statistically unbiased. For this reason, physical randomizing devices based on ‘chaotic’ physical phenomena, such as dice, shuffling playing cards and roulette wheels, have long been used for games and gambling as well as scientific purposes[8]. Later, methods were developed to quickly generate many pseudo-random numbers from a single ‘seed’ using deterministic algorithms, and these have many uses in modern digital electronic information systems[9]. Random phenomena such as photon noise, thermal noise in resistors, and frequency jitter in oscillators have been used as physical entropy sources for non-deterministic generators[10–17]. However, previous implementations of non-deterministic generators have been limited to much slower rates than pseudo-random generators due to limitations of the mechanisms for extracting bit sequences from physical noise without degrading statistical properties. Typical rates are 10 Mbps using electronic oscillator jitter[16] and 4 Mbps using quantum optical noise[14].

In this Letter, we report success in generating random bit sequences at rates up to 1.7 Gbps using high-bandwidth chaotic semiconductor lasers. Chaotic systems generate large-amplitude random signals from microscopic noise by nonlinear amplification and mixing mechanisms[18–23]. We make use of chaos in lasers to achieve efficient and stable generation of random bits at high frequencies. High-bandwidth chaotic lasers have previously been used to demonstrate the transmission of messages hidden in complex optical waveforms[24–26]. However, this is the first time that chaotic lasers have been used to demonstrate high-rate generation of random bit sequences with verified randomness.

The scheme for generating random bit sequences using chaotic lasers is shown in Fig. 1a. The scheme uses two semiconductor lasers with chaotic intensity oscillations. The output intensity of each laser is converted to an a.c. electrical signal by photodetectors, amplified and converted to a binary signal using a 1-bit analog-to-digital converter (ADC) driven by a fast clock. The ADC first converts the input analog signal into a binary signal by comparing with a threshold voltage, and then samples the binary signal at the rising edge of the clock. The binary bit signals obtained from the two lasers are combined by a logical exclusive-OR (XOR) operation to generate a single random bit sequence. No other digital post-processing is required.

An implementation of the laser scheme is shown in Fig. 1b. (see also Supplementary Information, Fig. S1). Single-mode distributed-feedback (DFB) lasers are prepared without standard optical isolators, to allow optical feedback from an external fibre reflector, which reflects a fraction of the light back into the laser, inducing high-frequency chaotic oscillations in the gigahertz regime[26–28].

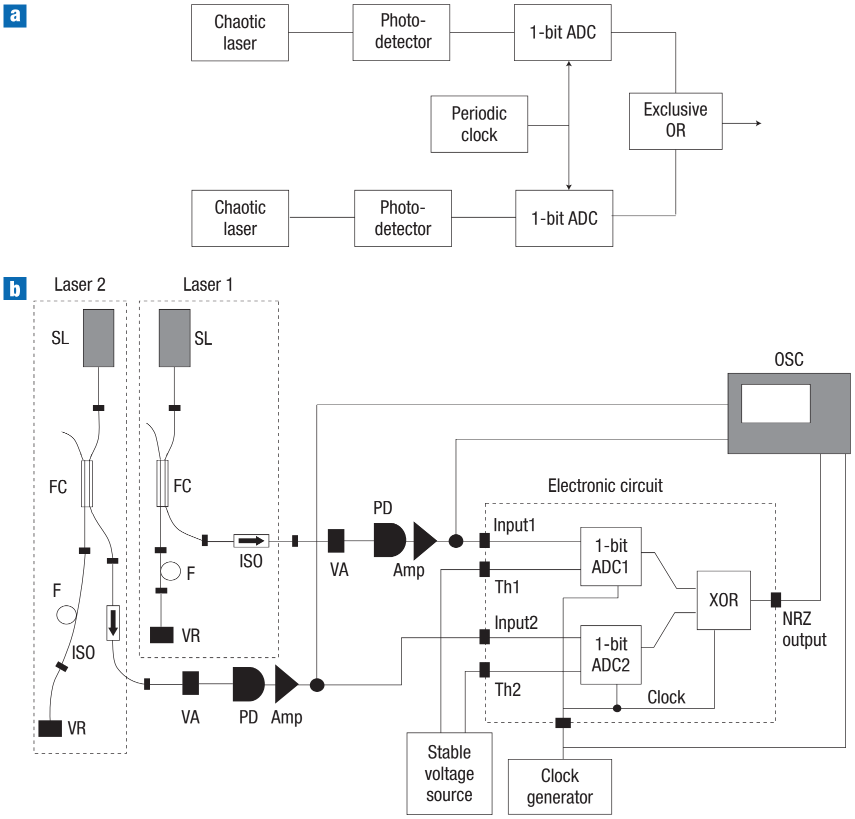

Figure 1 **Structure of random bit sequence generator using two chaotic lasers.** **a**, Schematic diagram. ADC, 1-bit analog-to-digital converter. **b**, Experimental setup. The lasers are the type used in optical fibre communications and are semiconductor distributed-feedback (DFB) lasers, operating at 1.5 μm wavelength and generating ∼1.5 mW of optical power. The lasers are prepared without standard optical isolators, to allow optical feedback from an external fibre reflector, which reflects a fraction of the light back into the laser, inducing high-frequency chaotic oscillations of the optical intensity. The amplitude of the optical feedback can be adjusted using the variable fibre reflector. Polarization-maintaining fibres are used for the optical fibre components. The intensity of the laser light output is converted to an electrical signal by a photodetector (12 GHz bandwidth) with a.c. coupling to remove the d.c. component. The signal is then amplified by an electronic amplifier (18 dB gain, 20 GHz bandwidth) and then converted to a binary digital signal by a 1-bit ADC. The ADC consists of a comparator and a D flip flop, which first converts the input analog signal into a binary level by comparing with the threshold voltage, and then samples the binary level at the rising edge of an external clock. The two independent binary digital signals obtained from the two lasers are then combined by an XOR operation. The output signal from the XOR operation is a stream of bits with a non-return-to-zero (NRZ) format that is suitable for high-speed data communications. Amp, electronic amplifier; F, optical fibre; FC, fibre coupler; ISO, fibre isolator; OSC, digital oscilloscope; PD, photodetector; SL, semiconductor laser; Th1,2, threshold voltages; VA, variable fibre attenuator; VR, variable fibre reflector; XOR, exclusive OR.

The procedure for realizing random bit generation at a particular bit rate is as follows. First we adjust the injection current, the length of the external cavity and the external feedback strength to put the lasers in a regime of high-bandwidth chaos. The parameters of the two lasers are then adjusted to ‘detune’ their chaotic oscillations and the threshold levels of the ADC adjusted to equalize the ratio of 0 and 1 at the XOR output.

An example of random bit generation at the maximum rate achievable with the lasers in this setup is shown in Fig. 2. The rate is 1.7 Gbps, corresponding to a clock with a frequency of 1.7 GHz. The temporal waveforms of the two chaotic laser outputs, the clock and the corresponding random bits sequences are shown in Fig. 2a. The signal at the bottom of Fig. 2a is the sequence of random bits output from the XOR operation, in a non-return-to-zero (NRZ) format that is suitable for high-speed data communications. The eye diagram of the output NRZ signal is shown in Fig. 2b. A visualization of the randomness of the bits is shown in Fig. 2c by plotting a single bit sequence as a 500 × 500 pattern of black and white dots (see also Supplementary Information, Video S1).

To evaluate the statistical randomness of digital bit sequences we used the standard statistical test suite for random number generators provided by the National Institute of Standard Technology (NIST) and the Diehard test suite[5–7]. The tests were performed using 1,000 instances of 1 Mbit sequences for NIST tests and using 74 Mbit sequences for Diehard tests. Bit sequences obtained from the experiment passed all of the NIST and Diehard tests. Typical results of the NIST tests are shown in Table 1. (Diehard results are shown in the Supplementary Information, Fig. S2).

To generate bit sequences that pass the statistical tests, control parameters of the laser (that is, external cavity length, injection current and optical feedback strength) were adjusted to detune the main periodic components of the chaotic oscillations, which are apparent in the autocorrelation characteristics (Fig. 3a,b). In other words, the delay time of the optical feedbacks ($\tau_{1,2}$) and the periods of the largest chaotic oscillation components ($\tau_{c1,c2}$) are made incommensurate with each other and with the clock period (τ_s). Bit sequences generated by a single laser exhibit recurrence features due to harmonic relations between the

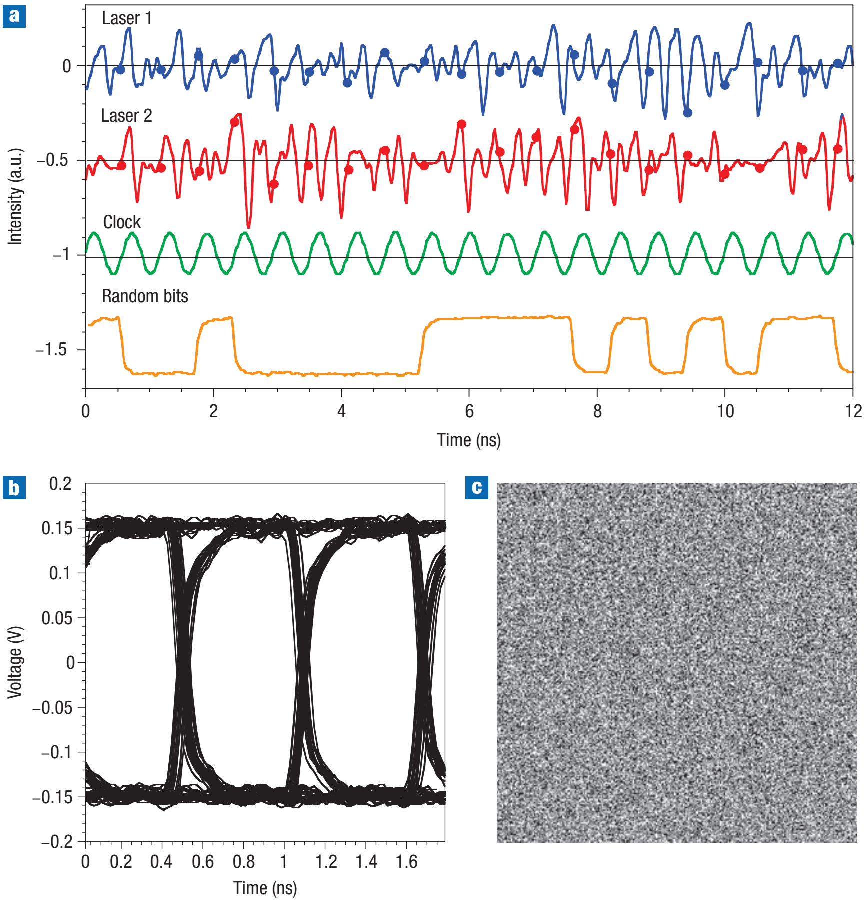

Figure 2 Typical output signals from an experimental system. a, Temporal waveforms of the laser output signals, the external clock and the corresponding random bit sequence. The threshold values for the ADCs are shown as solid lines. Solid dots mark points sampled at the rising edge of the clock. **b**, An eye diagram of the random bit signal. **c**, Random bit patterns in a two-dimensional plane. Bits 1 and 0 are converted into black and white dots, respectively, and placed from left to right (and from top to bottom); 500 × 500 bits are shown. The external cavity lengths of optical fibres in this case are set to 5.633 and 7.840 m for lasers 1 and 2, respectively, corresponding to feedback delay times (roundtrip) of 54.26 and 75.52 ns. The largest oscillation components of the two lasers, in the presence of optical feedback, are 3.07 and 2.86 GHz for lasers 1 and 2, respectively.

Table 1 Results of NIST Special Publication 800-22 statistical tests. For 'success' using 1000 samples of 1 Mbit data and significance level $\alpha = 0.01$, the *P*-value (uniformity of p-values) should be larger than 0.0001 and the proportion should be in the range of 0.99 ± 0.0094392. For the tests which produce multiple *P*-values and proportions, the worst case is shown.

Statistical test	*P*-value	Proportion	Result
Frequency	0.366918	0.9920	Success
Block frequency	0.639202	0.9900	Success
Cumulative sums	0.101311	0.9920	Success
Runs	0.223648	0.9920	Success
Longest run	0.603841	0.9890	Success
Rank	0.031012	0.9900	Success
FFT	0.274341	0.9910	Success
Nonperiodic templates	0.013760	0.9810	Success
Overlapping templates	0.893482	0.9910	Success
Universal	0.903338	0.9920	Success
Approximate entropy	0.880145	0.9920	Success
Random excursions	0.142248	0.9836	Success
Random excursions variant	0.068964	0.9869	Success
Serial	0.440975	0.9860	Success
Linear complexity	0.291091	0.9970	Success
Total			15

characteristic laser oscillation components and the clock. Combining the sequences from two lasers with incommensurate chaos produces better quality random sequences, with sufficient quality to pass the NIST and Diehard statistical tests. The use of optical-fibre components ensured stable oscillation conditions. Both the chaotic oscillations and sampling operations were stable with respect to mechanical and thermal perturbations, to the extent that the statistical properties of the sequences were maintained over many hours of continual operation. Stability of statistics could be improved further by adaptive control of the detection threshold while monitoring the 1/0 ratio.

The non-deterministic property of the bit sequences is assured by the amplification of microscopic laser noise by chaotic dynamics[29]. This can be confirmed by numerical analysis of the theoretical Lang–Kobayashi model for semiconductor lasers with optical feedback[27,28], and stochastic noise consistent with the experimental noise power spectrum (Fig. 3d). The effect of the noise in the chaotic lasers is such that even lasers starting in the same state, or lasers whose past bit sequences are identical, generate different sequences in the future. The entropy of possible future sequences is a measure of unpredictability. At bit rates up to a few gigabits per second, the entropy generation rate

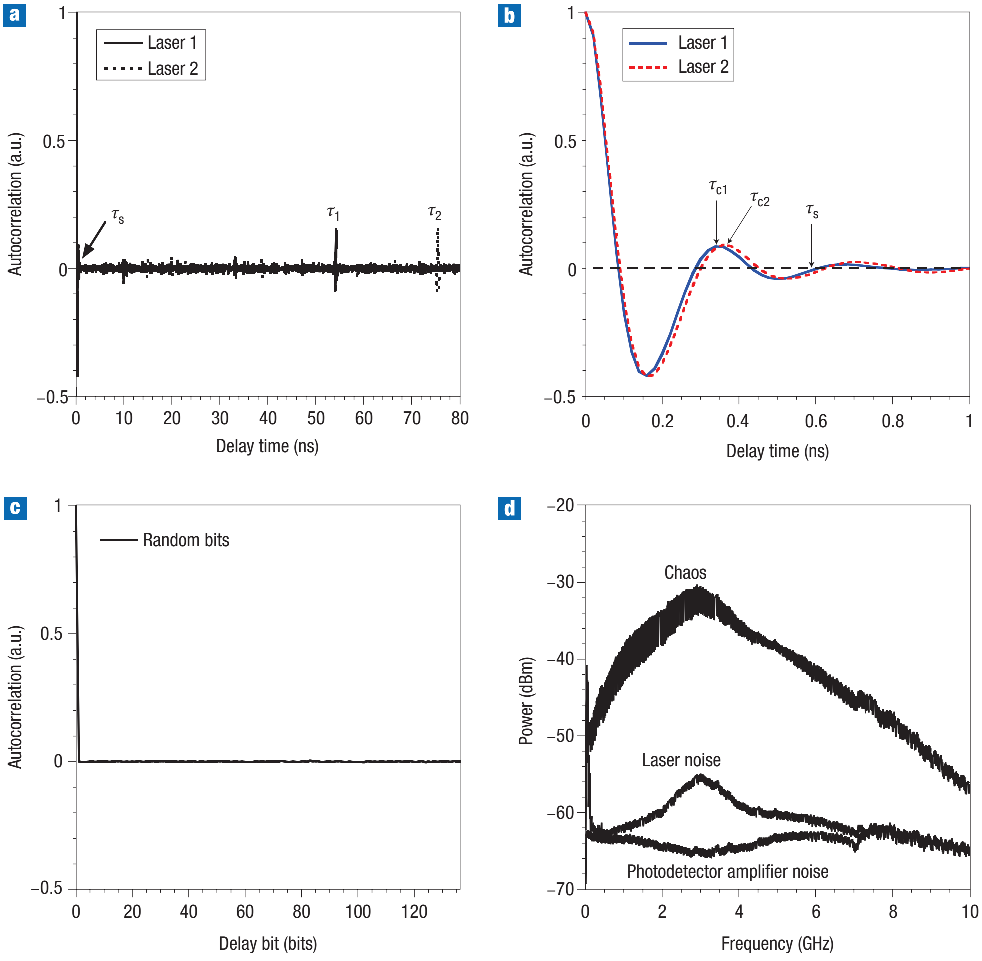

Figure 3 Autocorrelation and spectral characteristics. a, Autocorrelation functions of the chaotic waveforms of the two lasers. τ_1 and τ_2 correspond to the feedback times of the external cavities. The values of $\tau_{1,2}$ can be controlled by adjusting the length of the external fibre cavity. τ_s, clock period. **b**, Enlargement of the short-time autocorrelation. τ_{c1} and τ_{c2} correspond to the largest component of the chaotic oscillation. The values of $\tau_{c1,c2}$ can be controlled by adjusting the injection current. The correlation peaks decay rapidly over a few periods due to the strongly chaotic dynamics. The following conditions hold (i) $\tau_{1,2} > \tau_s > \tau_{c1,c2}$ (ii) $l\tau_1 \neq m\tau_2 \neq n\tau_s$ for any low-order integers l, m, n. **c**, Autocorrelation function of random bit sequence output from the XOR device. One bit corresponds to $\tau_s = 0.588$ ns ($1/\tau_s = 1.7$ GHz). The timescale of Fig. 3c corresponds to the timescale of Fig. 3a. It can be seen there is no autocorrelation corresponding to τ_1, τ_2, or any other delay. **d**, Radio-frequency spectra for the chaotic oscillation, laser noise and photodetector-amplifier noise. The laser noise is observed when the laser has no external optical feedback.

can exceed the bit rate, ensuring the unpredictability of the bits in the steady state of continuous generation (see Supplementary Information, Figs S3,S4,S5 for details).

In comparison, we found that the intrinsic laser noise alone is not sufficient for random bit generation. Laser noise obtained using the same ADC system when the optical feedback is reduced to zero (Fig. 3d) results in sequences with biased ratios of 0 and 1. This can be explained by the fact that the amplitude of the noise is small with respect to the variation of the threshold level (see Supplementary Information, Fig. S6). In this sense, the large-amplitude chaotic oscillations induced by optical feedback are more effective than non-chaotic laser noise for generating random bit sequences in this system.

Sequences generated at rates between 1.0 and 1.7 Gbps passed the NIST statistical tests, but sequences generated at higher rates did not. The maximum rate is limited by the bandwidth of the chaos. Faster rates can be achieved by schemes that enhance the bandwidth of the chaos in the lasers, such as optical injection[30]. We confirmed that sequences that passed both the NIST and Diehard randomness tests were obtainable at rates up to 6.2 Gbps using optical injection to enhance the bandwidth of chaos beyond 10 GHz. Design of laser schemes to achieve higher rates of 10 Gbps and more, and their integration in compact photonic modules, is a promising direction for future study.

In conclusion, we have demonstrated that continuous streams of random bit sequences that pass standard tests of randomness are generated at fast rates of up to 1.7 Gbps by directly sampling the output of two chaotic semiconductor lasers. The rate that we obtained is faster than that of any previously reported devices for physical generation of bit sequences with verified randomness, and demonstrates the large potential for improvements in performance of random number generators by harnessing chaotic laser devices as physical entropy sources.

Received 23 June 2008; accepted 16 October 2008; published 23 November 2008.

References

1. Eastlake, D., Schiller, J., & Crocker, S. Randomness requirements for security. Available at http://tools.ietf.org/html/rfc4086 RFC4086 2005.
2. Security requirements for cryptographic modules. Available at http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf FIPS 140-2 (2001).

3. Metropolis, N., & Ulam, S. The Monte Carlo method. *J. Am. Statist. Assoc.* **44,** 335–341 (1949).
4. Gisin, N., Robordy, G., Tittel, W., & Zbinden, H. Quantum cryptography. *Rev. Modern Phys.* **74,** 145–195 (2002).
5. Marsaglia, G. DIEHARD: A battery of tests of randomness. Available at http://stat.fsu.edu/ geo (1996).
6. Rukhin, A. *et al*. A statistical test suite for random and pseudorandom number generators for cryptographic applications. National Institute of Standards and Technology, Special Publication 800-22 (2001).
7. Kim, S. J., Umeno, K. & Hasegawa, A. Corrections of the NIST statistical test suite for randomness. arXiv:nlin.CD/0401040v1 (2004).
8. Galton, F. Dice for statistical experiments. *Nature* **42,** 13–14 (1890).
9. Knuth, D. *The Art of Computer Programming: Volume 2: Seminumerical Algorithms* 3rd edn (Addison-Wesley Professional, 1996).
10. Kelsey, J. *Entropy and Entropy Sources in X9.82* (NIST, 2004).
11. Schindler, W. & Killmann, W. Evaluation criteria for true (physical) random number generators used in cryptographic applications. *CHES 2002, Lecture Notes in Computer Science* **2523,** 431–449 (2002).
12. Jun, B. & Kocher, P. The Intel random number generator. White paper prepared for Intel Corporation, Cryptography Research Inc. Available at http://www.cryptography.com/resources/whitepapers/IntelRNG.pdf. (1999).
13. Holman, W. T., Connelly, J. A. & Dowlatabadi, A. B. An integrated analog/digital random noise source. *IEEE Trans. Circuits and Systems I* **44,** 521–528 (1997).
14. Dynes, J. F., Yuan, Z. L., Sharpe, A. W. & Shields, A. J. A high speed, post-processing free, quantum random number generator, arxiv/0807.4111v1 (July 2008).
15. Cortigiani, F., Petri, C., Rocchi, S. & Vignoli, V. Very high-speed true random noise generator. *The 7th IEEE International Conference on Electronics, Circuits and Systems, 2000 (ICECS 2000)* **1,** 120–123 (2000).
16. Bucci, M., Germani, L., Luzzi, R., Trifiletti, A. & Varanouvo, M. A high-speed oscillator-based truly random number source for cryptographic applications on a Smart Card IC. *IEEE Trans. Comput.* **52,** 403–409 (2003).
17. Tokunaga, C., Blaauw, D. & Mudge, T. True random number generator with a metastability-based quality control. *IEEE J. Solid-State Circuits* **43,** 78–85 (2008).
18. Ornstein, D. S. Ergodic theory, randomness and 'chaos'. *Science* **243,** 182–187 (1989).
19. Wolfram, S. Random sequence generation by cellular automaton. *Adv. Appl. Math.* **7,** 123–169 (1986).
20. Stojanovski, T. & Kocarev, L. Chaos-based random number generators-part I: analysis [cryptography]. *IEEE Trans. Circ. Syst. I: Fund. Theory Appl.* **48,** 281–288 (2001).
21. Pappu, R., Recht, B., Taylor, J. & Gershenfeld, N. Physical one-way functions. *Science* **297,** 2026–2030 (2002).
22. Gleeson, J. T. Truly random number generator based on turbulent electroconvection. *Appl. Phys. Lett.* **81,** 1949–1951 (2002).
23. Callegari, S., Rovatti, R. & Setti, G. Embeddable ADC-based true random number generator for cryptographic applications using nonlinear signal processing and chaos. *IEEE Trans. Signal Process.* **53,** 793–805 (2005).
24. VanWiggeren, G. D. & Roy, R. Communication with chaotic lasers. *Science* **279,** 1198–1200 (1998).
25. Argyris, A. *et al*. Chaos-based communications at high bit rates using commercial fibre-optic links. *Nature* **438,** 343–346 (2005).
26. Liu, J. M., Chen, H. F. & Tang, S. Synchronized chaotic optical communications at high bit rates. *IEEE J. Quant. Electron.* **38,** 1184–1196 (2002).
27. Lang, R. & Kobayashi, K. External optical feedback effects on semiconductor injection laser properties. *IEEE J. Quant. Electron.* **16,** 347–355 (1980).
28. Uchida, A., Liu, Y. & Davis, P. Characteristics of chaotic masking in synchronized semiconductor lasers. *IEEE J. Quant. Electron.* **39,** 963–970 (2003).
29. Bracikowski, C., Fox, R. F. & Roy, R. Amplification of intrinsic noise in a chaotic multimode laser system. *Phys. Rev. A* **45,** 403–408 (1992).
30. Uchida, A., Heil, T., Liu, Y., Davis, P. & Aida, T. High-frequency broad-band signal generation using a semiconductor laser with a chaotic optical injection. *IEEE J. Quant. Electron.* **39,** 1462–1467 (2003).

Supplementary Information accompanies this paper at www.nature.com/naturephotonics.

Acknowledgements

The authors thank Y. Tonomura, N. Ueda, S. Makino, K. Nakazawa, M. Miyoshi and J. Muramatsu of NTT Communication Science Laboratories and S. Katagiri of Doshisha University for their support and encouragement. A.U. acknowledges support from NTT Corporation, Support Centre for Advanced Telecommunications Technology Research, and Grants-in-Aid for Scientific Research from the Japan Society for the Promotion of Science. We thank K. Umeno, S.-J. Kim and H. Terai for advice on the statistical evaluation of random numbers. We are grateful to I. Fischer, L. Larger, C. R. Mirasso and R. Roy for helpful discussions on laser chaos.

Author information

Reprints and permission information is available online at http://npg.nature.com/reprintsandpermissions/. Correspondence and requests for materials should be addressed to A.U.