Fast random bit generation with bandwidth-enhanced chaos in semiconductor lasers

Kunihito Hirano,[1] Taiki Yamazaki,[2] Shinichiro Morikatsu,[2] Haruka Okumura,[2] Hiroki Aida,[2] Atsushi Uchida, [2,*] Shigeru Yoshimori,[1] Kazuyuki Yoshimura,[3] Takahisa Harayama,[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

**auchida@mail.saitama-u.ac.jp*

Abstract: We experimentally demonstrate random bit generation using multi-bit samples of bandwidth-enhanced chaos in semiconductor lasers. Chaotic fluctuation of laser output is generated in a semiconductor laser with optical feedback and the chaotic output is injected into a second semiconductor laser to obtain a chaotic intensity signal with bandwidth enhanced up to 16 GHz. The chaotic signal is converted to an 8-bit digital signal by sampling with a digital oscilloscope at 12.5 Giga samples per second (GS/s). Random bits are generated by bitwise exclusive-OR operation on corresponding bits in samples of the chaotic signal and its time-delayed signal. Statistical tests verify the randomness of bit sequences obtained using 1 to 6 bits per sample, corresponding to fast random bit generation rates from 12.5 to 75 Gigabit per second (Gb/s) (= 6 bit × 12.5 GS/s).

OCIS codes: (140.1540) Chaos; (190.3100) Instabilities and chaos; (140.5960) Semiconductor lasers; (060.4510) Optical communications.

References and links

1. D. Eastlake, J. Schiller, and S. Crocker, "Randomness requirements for security," RFC4086 (2005) http://tools.ietf.org/html/rfc4086
2. Security requirements for cryptographic modules. FIPS 140–2 (2001) http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
3. N. Gisin, G. Robordy, W. Tittel, and H. Zbinden, "Quantum Cryptography," Rev. Mod. Phys. **74**(1), 145–195 (2002).
4. N. Metropolis, and S. Ulam, "The Monte Carlo method," J. Am. Stat. Assoc. **44**(247), 335–341 (1949).
5. D. Knuth, "*The Art of Computer Programming,*" Volume 2: Seminumerical Algorithms (3rd Edition), Addison-Wesley Professional (1996).
6. W. T. Holman, J. A. Connelly, and A. B. Dowlatabadi, "An integrated analog/digital random noise source," IEEE Trans. Circuits Syst. I **44**(6), 521–528 (1997).
7. J. T. Gleeson, "Truly random number generator based on turbulent electroconvection," Appl. Phys. Lett. **81**(11), 1949 (2002).
8. M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanouvo, "A high-speed oscillator-based truly random number source for cryptographic applications on a Smart Card IC," IEEE Trans. Comput. **52**(4), 403–409 (2003).
9. J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, "A high speed, post-processing free, quantum random number generator," Appl. Phys. Lett. **93**(3), 1–3 (2008).
10. B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, "High-speed quantum random number generation by measuring phase noise of a single-mode laser," Opt. Lett. **35**(3), 312–314 (2010).
11. A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, "Fast physical random bit generation with chaotic semiconductor lasers," Nat. Photonics **2**(12), 728–732 (2008).
12. T. E. Murphy, and R. Roy, "The world's fastest dice," Nat. Photonics **2**(12), 714–715 (2008).
13. K. Hirano, K. Amano, A. Uchida, S. Naito, M. Inoue, S. Yoshimori, K. Yoshimura, and P. Davis, "Characteristics of fast physical random bit generation using chaotic semiconductor lasers," IEEE J. Quantum Electron. **45**(11), 1367–1379 (2009).

#121087 - $15.00 USD Received 7 Dec 2009; revised 12 Feb 2010; accepted 14 Feb 2010; published 3 Mar 2010

14. T. Honjo, A. Uchida, K. Amano, K. Hirano, H. Someya, H. Okumura, K. Yoshimura, P. Davis, and Y. Tokura, "Differential-phase-shift quantum key distribution experiment using fast physical random bit generator with chaotic semiconductor lasers," Opt. Express **17**(11), 9053–9061 (2009).
15. I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, "Ultrahigh-speed random number generation based on a chaotic semiconductor laser," Phys. Rev. Lett. **103**(2), 1–4 (2009).
16. Y. Takiguchi, K. Ohyagi, and J. Ohtsubo, "Bandwidth-enhanced chaos synchronization in strongly injection-locked semiconductor lasers with optical feedback," Opt. Lett. **28**(5), 319–321 (2003).
17. A. Uchida, T. Heil, Y. Liu, P. Davis, and T. Aida, "High-frequency broad-band signal generation using a semiconductor laser with a chaotic optical injection," IEEE J. Quantum Electron. **39**(11), 1462–1467 (2003).
18. F. Y. Lin, and J. M. Liu, "Nonlinear dynamical characteristics of an optically injected semiconductor laser subject to optoelectronic feedback," Opt. Commun. **221**, 173–180 (2003).
19. A. Wang, Y. Wang, and H. He, "Enhancing the bandwidth of the optical chaotic signal generated by a semiconductor laser with optical feedback," IEEE Photon. Technol. Lett. **20**(19), 1633–1635 (2008).
20. H. Someya, I. Oowada, H. Okumura, T. Kida, and A. Uchida, "Synchronization of bandwidth-enhanced chaos in semiconductor lasers with optical feedback and injection," Opt. Express **17**(22), 19536–19543 (2009).
21. G. D. VanWiggeren, and R. Roy, "Communication with chaotic lasers," Science **279**(5354), 1198–1200 (1998).
22. J.-P. Goedgebuer, L. Larger, and H. Porte, "Optical cryptosystem based on synchronization of hyperchaos generated by a delayed feedback tunable laser diode," Phys. Rev. Lett. **80**(10), 2249–2252 (1998).
23. A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. García-Ojalvo, C. R. Mirasso, L. Pesquera, and K. A. Shore, "Chaos-based communications at high bit rates using commercial fibre-optic links," Nature **437**(7066), 343–346 (2005).
24. F.-Y. Lin, and J.-M. Liu, "Chaotic lider," IEEE J. Sel. Top. Quantum Electron. **10**(5), 991–997 (2004).
25. J. Ohtsubo, "*Semiconductor Lasers, -Stability, Instability and Chaos-*," Second Ed., Springer-Verlag, Berlin Heidelberg (2005).
26. A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, and M. Levenson, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," National Institute of Standards and Technology, Special Publication 800–22, 2001; Revision 1, August 2008. http://csrc.nist.gov/publications/nistpubs/800-22-rev1/SP800-22rev1.pdf
27. S. J. Kim, K. Umeno, and A. Hasegawa, "Corrections of the NIST statistical test suite for randomness," arXiv:nlin.CD/0401040v1, 2004.
28. G. Marsaglia, DIEHARD: A battery of tests of randomness. http://stat.fsu.edu/ geo, 1996.
29. I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, "An optical ultrafast random bit generator," Nat. Photonics **4**(1), 58–61 (2010).

1. Introduction

Random numbers are widely used in information security schemes as codes, keys and challenges to ensure confidentiality, authenticity and integrity of information [1,2]. Quantum cryptography systems require the generation of truly random numbers to ensure that detection parameters are unpredictable [3]. Random numbers are also used for sampling in complex numerical computations [4]. Generators of random numbers can be classified into two categories: pseudo random-number generators and physical random-number generators. Pseudo-random numbers are generated from a single random seed using deterministic algorithms, and these are used in modern digital electronic information systems [5]. Sequences of pseudo-random numbers generated deterministically from the same seed will be identical, and this can cause serious problems for applications in information security systems. For this reason, physically random processes are often used as entropy sources in random number generators [6–10]. Random phenomena such as photon noise, thermal noise in resistors and frequency jitter of oscillators have been used as physical entropy sources for non-deterministic random bit generation in combination with deterministic pseudo-random bit generators. However, non-deterministic generators have been limited to much slower rates than pseudo-random generators due to limitations of the mechanisms for extracting bits from physical noise [8–10].

Recently, we have experimentally demonstrated that continuous streams of random bit sequences that pass standard tests of randomness can be generated at fast rates of up to 1.7 Gigabit per second (Gb/s) *in real time* by directly sampling the output of two chaotic semiconductor lasers with one-bit analog-digital converters [11–13]. This rate is not only much faster than any previous methods, but also it shows that the rate of bit generation in physical random generators can be comparable to that in digital pseudo-random generators. Moreover, the use of semiconductor lasers is particularly compatible with delivery of random bits by optical fiber systems. Our physical random bit generator has also been applied to a

#121087 - $15.00 USD Received 7 Dec 2009; revised 12 Feb 2010; accepted 14 Feb 2010; published 3 Mar 2010

gigahertz-clocked differential-phase-shift quantum key distribution system for random phase modulation of optical pulses [14]. Very recently, Reidler and associates have shown that sequences passing statistical tests of randomness can be achieved at higher bit rates from a single chaotic semiconductor laser by extracting more than one bit per sample in off-line processing of experimental chaotic laser time series [15]. Specifically, a rate equivalent to 12.5 Gb/s was achieved by extracting 5 bits from the difference in 8-bit samples acquired at 2.5 GHz sampling rate. It is an ongoing challenge to increase the speed of physical random number generators and to develop bit extraction mechanisms which increase the random bit generation capacity.

One promising approach to increasing the generation speed of random bit generators is a technique for bandwidth enhancement of optical chaos in semiconductor lasers [16–20]. The bit rate of generated random sequences is limited by the dominant oscillation frequency of chaotic waveforms, which is around the relaxation oscillation frequency of several GHz. To achieve significantly higher rates it is necessary to largely enhance the bandwidth of chaotic waveforms. Several studies on the bandwidth enhancement of chaos in optically coupled semiconductor lasers have been reported [16–20], aimed at applications in chaos communications [21–23] and chaotic lidar [24].

In this paper, we experimentally demonstrate the generation of random bits by using bandwidth-enhanced chaos in semiconductor lasers. Chaotic fluctuation of laser output is generated in a semiconductor laser with optical feedback and the chaotic output is injected into a second semiconductor laser for bandwidth enhancement. We demonstrate the enhancement of the chaos bandwidth up to 16 GHz, and random bit generation at rates equivalent to up to 75 Gb/s with multi-bit sampling at 12.5 Giga samples per second (GS/s).

2. Experimental setup

Figure 1 shows our experimental setup for the scheme of fast physical random bit generation. We used two distributed-feedback (DFB) semiconductor lasers mounted in butterfly packages with optical fiber pigtails (NTT Electronics, NLK1C5GAAA, the optical wavelength of 1547 nm), developed for optical fiber communications. One laser (referred to as Laser 1) was used for the generation of chaotic intensity fluctuations induced by optical feedback. The other laser (referred to as Laser 2) was used for the bandwidth enhancement of chaotic waveforms. The injection current and the temperature of the semiconductor lasers were adjusted by a current-temperature controller (Newport, 8000-OPT-41-41) with stability of 0.01 mA/hour and 0.01 K/hour, respectively. The optical wavelength of the lasers was precisely controlled by the temperature of the laser with control coefficient of 0.097 nm/K. The lasing thresholds of the injection current I_{th} for solitary Laser 1 and 2 were 9.43 and 9.31 mA, respectively. Both Laser 1 and 2 were prepared without standard optical isolators, to allow optical feedback and injection. Laser 1 was connected to a fiber coupler and a variable fiber reflector which reflects a fraction of the light back into the laser, inducing high-frequency chaotic oscillations of the optical intensity. The amount of the optical feedback light was adjusted by the variable fiber reflector. The fiber length between Laser 1 and the variable fiber reflector was 4.55 m, corresponding to a feedback delay time (round-trip) of 43.8 ns. On the other hand, there was no optical feedback for Laser 2. Polarization maintaining fibers were used for all the optical fiber components.

A portion of the chaotic Laser 1 beam was injected into Laser 2. Two optical isolators were used to achieve one-way coupling from Laser 1 to Laser 2. The wavelengths of Laser 1 and 2 were precisely adjusted in order to generate bandwidth-enhanced chaotic output of Laser 2, as described in the following section. A portion of Laser 2 output was extracted by a fiber coupler, and divided into two beams by another fiber coupler. An extra optical fiber (1-meter length) was inserted into one of the optical paths after the two beams were divided, so that a chaotic waveform and its time-delayed signal (5.0 nanosecond delay) could be detected by two photodetectors (New Focus, 1434, 25 GHz bandwidth). The converted electronic signal at the photodetectors were amplified by electronic amplifiers (New Focus, 1422-LF, 20 GHz bandwidth) and sent to a digital oscilloscope (Tektronix, DSA72004, 20 GHz

#121087 - $15.00 USD Received 7 Dec 2009; revised 12 Feb 2010; accepted 14 Feb 2010; published 3 Mar 2010

bandwidth, 50 GigaSamples/s) and a radio-frequency (RF) spectrum analyzer (Agilent, N9010A-526, 26.5 GHz bandwidth) to observe temporal waveforms and the corresponding RF spectra, respectively. The optical wavelength of the lasers was measured by an optical spectrum analyzer (Advantest, Q8384).

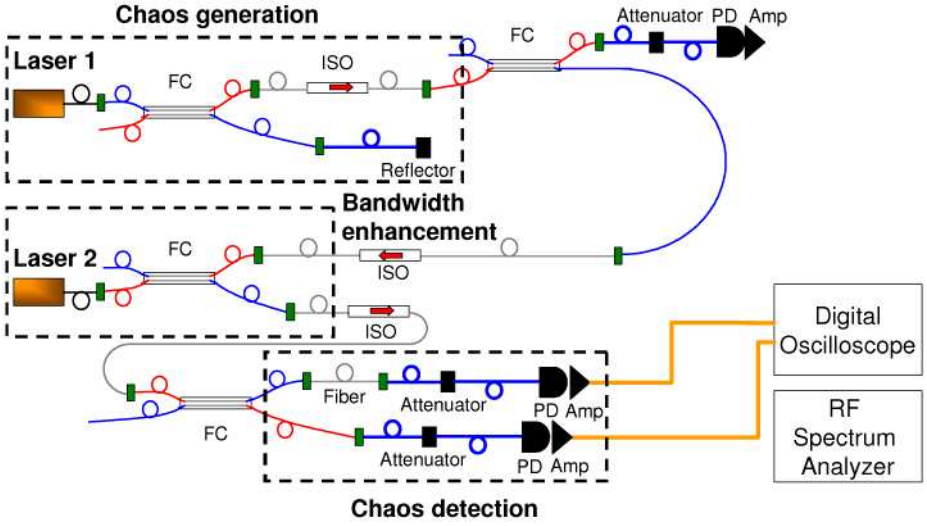

Fig. 1. Experimental setup for random bit generation with chaotic lasers. Amp, electronic amplifier; FC, fiber coupler ; ISO, optical isolator; PD, photodetector.

3. Experimental results

3.1 Bandwidth enhancement of chaos

We set the relaxation oscillation frequencies to be 6.5 GHz for both Laser 1 and 2 by adjusting the injection current of the lasers. These values were close to the maximum relaxation oscillation frequencies that can be observed for solitary lasers in the experiment. The injection currents for Laser 1 and 2 were set to 58.50 mA ($6.20I_{th}$) and 59.00 mA ($6.34I_{th}$), respectively. To enhance the bandwidth of chaos, we detuned the optical wavelength of Laser 2 to the positive direction with respect to that of Laser 1, i.e., we set the optical wavelength to be 1547.585 nm for Laser 1 and 1547.677 nm for Laser 2, by controlling the temperature of the two lasers. The optical wavelength for Laser 2 was shifted to 1547.718 nm due to the presence of the optical injection from Laser 1. The optical wavelength detuning was defined as $\Delta\lambda = \lambda_2 - \lambda_1$, where λ_1 and λ_2 indicate the optical wavelength of Laser 1 and 2 in the presence of the optical injection, respectively. $\Delta\lambda$ was set to 0.133 nm (16.6 GHz in frequency), which corresponds to the positive detuning condition in the literature [25]. At this condition, no injection locking was achieved between Laser 1 and 2, where injection locking was defined as the matching of optical wavelengths between the two lasers due to the coherent unidirectional coupling. The existence of the frequency component corresponding to the optical wavelength detuning is crucial for the bandwidth enhancement of the laser chaos [20]; it results in nonlinear frequency mixing between the optical wavelength detuning and the relaxation oscillation frequency of the laser. When the detuning is small enough so that injection locking is achieved, the bandwidth of Laser 2 is exactly matched with that of Laser 1, since synchronization of temporal waveforms is obtained between the Laser 1 and 2 under the injection locking condition [20].

Figures 2(a) and 2(b) show the RF spectra of Laser 1 and 2. The RF spectra in Figs. 2(a) and 2(b) show that bandwidth enhancement of Laser 2 by the optical injection of the Laser 1 output, where the center frequencies of Laser 1 and 2 are 6.6 and 16.1 GHz, respectively. We define the bandwidth of the chaotic signals as the frequency band starting at zero frequency and containing 80% of spectrum power [18–20]. The bandwidth of Laser 1 and 2 are 9.5 and

#121087 - $15.00 USD Received 7 Dec 2009; revised 12 Feb 2010; accepted 14 Feb 2010; published 3 Mar 2010

16.1 GHz, respectively. The bandwidth enhancement of chaotic signals is achieved up to approximately 16 GHz by optical injection of chaotic signal. It can also be seen that the RF spectrum of the output of Laser 2, shown in Fig. 2(b), is much flatter than that of Laser 1 in Fig. 2(a). Flatness of the RF spectrum is advantageous for the generation of random bit sequences [13]. The enhancement of chaos bandwidth up to 16 GHz enables us to generate random bit sequences by sampling at the rate of 12.5 GS/s, which is much faster than the previously reported sampling rates of 1.7 and 2.5 GS/s [11,15].

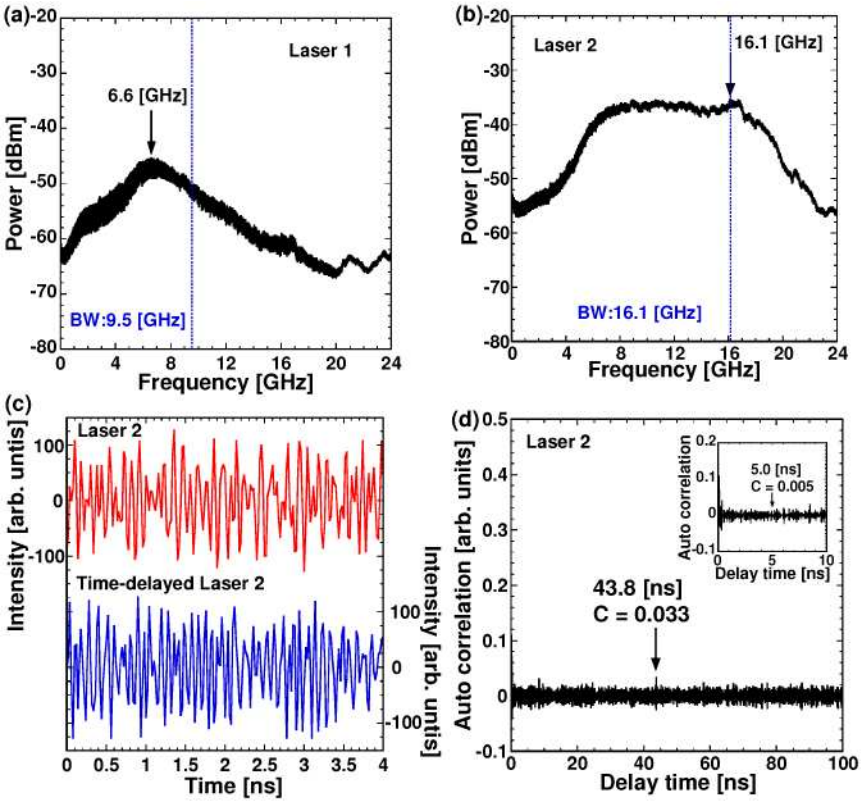

Fig. 2. (a) RF spectrum of Laser 1, (b) RF spectrum of Laser 2, (c) temporal waveforms of Laser 2 output and the same output optically delayed in time (5.0 ns delay), and (d) autocorrelation function of the temporal waveform of Laser 2 output. The inset is the enlargement of (d). (a), (b) BW: bandwidth.

Figure 2(c) shows the temporal waveform of the Laser 2 output and the same output optically delayed by 5.0 ns, as detected by the two photodetectors. These two chaotic signals are used for the generation of random bit sequences. The temporal waveforms of the AC-signals from the photodetectors are detected using a dual-channel 8-bit oscilloscope sampling at 12.5 GS/s, with the 8-bit range adjusted symmetrically to ±2 standard-deviations of the signal amplitude. The match between the signal amplitudes and the range of the 8-bit detectors in the oscilloscope was adjusted using the optical attenuators.

The autocorrelation function of the Laser 2 output is shown in Fig. 2(d). The peak of the autocorrelation appears at 43.8 ns, corresponding to the round-trip time of the external cavity for Laser 1. The peak value of the autocorrelation function at 43.8ns is only 0.033, showing that periodicity due to the external cavity of the Laser 1 is suppressed in the Laser 2 output. We note that the correlation is 0.005 at the time of 5.0 ns corresponding to the delay between the two detected signals, as shown in the inset of Fig. 2(d).

#121087 - $15.00 USD Received 7 Dec 2009; revised 12 Feb 2010; accepted 14 Feb 2010; published 3 Mar 2010

3.2 Generation of random bits

We generate random bits using two chaotic waveforms; the output of Laser 2 and the output of Laser 2 optically delayed by 5.0 ns. The two chaotic optical signals are detected by AC-coupled photodetectors, amplified and converted to digital 8-bit signals by a dual channel oscilloscope sampling at 12.5 GS/s per channel. Corresponding pairs of bits in the two 8-bit digital signals are combined by bitwise exclusive-OR (XOR) operation, giving a single 8-bit digital signal. A subset of m least significant bits (LSBs) from each sample are then selected and interleaved to generate a single bit sequence [15], which can be specified as follows:

$$\ldots, s_m(t), s_{m-1}(t), \ldots, s_1(t), s_m(t+1), s_{m-1}(t+1), \ldots s_1(t+1), \ldots$$

where $s_k = 0$ or 1 $(k = 1, 2, \ldots, m)$ is the k-th LSB of the selected m LSBs. The method is illustrated in Fig. 3.

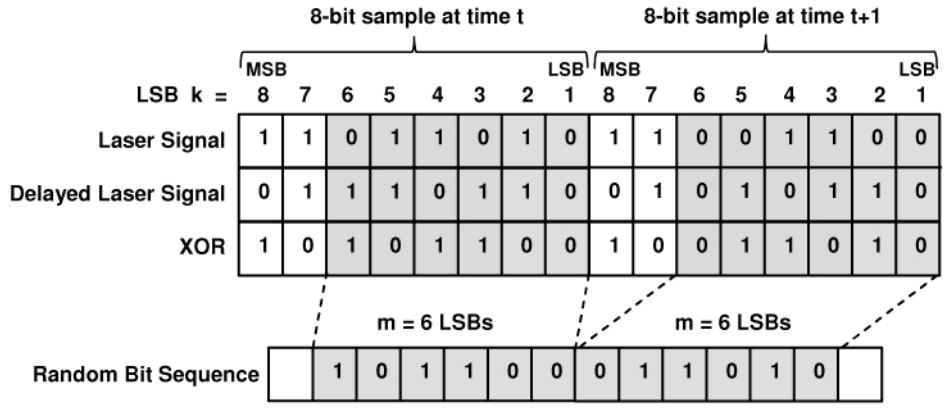

Fig. 3. Method for generating a random bit sequence using multiple (m = 1,…, 8) significant bits. Example for m = 6. LSB, least significant bit; MSB, most significant bit; XOR, exclusive-OR operation.

In our experimental system, the XOR operation and bit interleave are done off-line after acquisition by the oscilloscope. The record length of each continual data frame acquired by the oscilloscope is 1M samples. 1000 frames are recorded for each channel to obtain sufficient data for the statistical tests of randomness.

Figure 4 shows an example of a long bit sequence generated by the laser system. The bit sequence is plotted in a two-dimensional plane. Bits "1" and "0" are converted into white and black dots, respectively, and placed from left to right (and from top to bottom). 500 by 500 bits are shown in Fig. 4. It can be seen that there are no obvious patterns and that the ratio of 1 and 0 is roughly equal, as we would expect from a random generation process. The randomness of bit sequences was tested using a standard statistical test suite for random number generators provided by the National Institute of Standard Technology (NIST), known as NIST Special Publication 800-22 (NIST SP 800-22) [26,27]. The NIST SP 800-22 test consists of 15 statistical tests, as shown in Table 1. The tests are performed using 1000 samples of 1 Mbit sequences and the significance level $\alpha = 0.01$ [26]. We also use another statistical test suite for random number generators, the so-called "Diehard" tests [28]. The Diehard test suite consists of 18 statistical tests, as shown in Table 2. The Diehard tests are performed using 74 Mbit sequences and significance level of $\alpha = 0.01$.

Typical results of the NIST tests are shown in Table 1, and typical results of the Diehard tests are shown in Table 2, for a set of sequences generated using 6 consecutive LSBs (see Fig. 3). The laser parameters used to generate the sequences correspond to the parameters used for Fig. 2. We confirmed that random bit sequences obtained from the bandwidth-enhanced chaos by 8-bit sampling at 12.5 GS/s are sufficiently random that they pass all the statistical tests of both NIST SP 800-22 and Diehard. Moreover, sequences obtained by

#121087 - $15.00 USD Received 7 Dec 2009; revised 12 Feb 2010; accepted 14 Feb 2010; published 3 Mar 2010

interleaving up to 6 consecutive LSBs at each sample also passed the statistical tests of randomness. These results correspond to random bit generation rates from 12.5 to 75 Gb/s (= 6 bit × 12.5 GS/s). We also found that, for the sequences generated using only one of the 8 bits at each sample, 7 of the 8 significant bits (i.e., all bits except MSB) passed statistical tests of randomness (see Sec. 4.3).

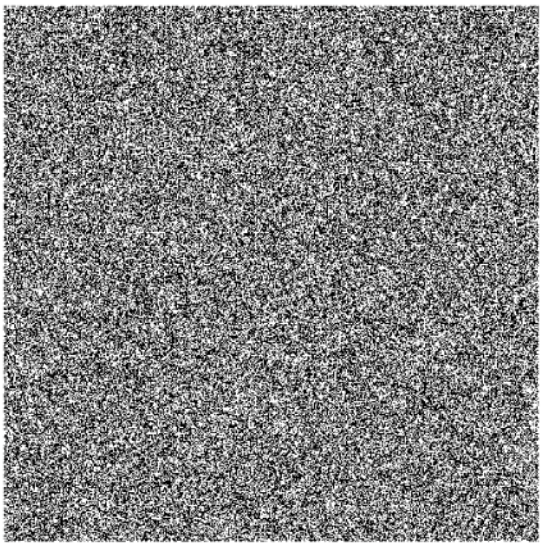

Fig. 4. Example of random bit sequence plotted in two-dimensional plane. Bits "1" and "0" are converted into white and black dots, respectively, and placed from left to right (and from top to bottom). 500 by 500 bits are shown.

Table 1. Example of results of statistical test suite NIST SP 800-22 for a set of 1000 sequences generated using 6 LSBs. Each sequence is 1 Mbit. Significance level: α = 0.01. To pass the tests, the P-value of the uniformity of p-values should be larger than 0.0001, and the proportion of sequences satisfying p-value > α for 1000 samples should be in the range of 0.99 ± 0.0094392 [26]. For tests which produce multiple P-values and proportions, the worst case is shown.

STATISRICAL TEST	P-VALUE	PROPARATION	RESULT
frequency	0.219006	0.9880	SUCCESS
block-frequency	0.000387	0.9860	SUCCESS
cumulative-sums	0.572847	0.9870	SUCCESS
runs	0.000550	0.9860	SUCCESS
longest-run	0.917870	0.9900	SUCCESS
rank	0.440975	0.9860	SUCCESS
fft	0.933472	0.9860	SUCCESS
nonperiodic-template	0.013856	0.9810	SUCCESS
overlapping-template	0.777265	0.9890	SUCCESS
universal	0.518106	0.9880	SUCCESS
apen	0.087682	0.9910	SUCCESS
random-excursions	0.013411	0.9868	SUCCESS
random-excursions-variant	0.112047	0.9851	SUCCESS
serial	0.162606	0.9870	SUCCESS
linear-complexity	0.989425	0.9900	SUCCESS
Total			15

#121087 - $15.00 USD Received 7 Dec 2009; revised 12 Feb 2010; accepted 14 Feb 2010; published 3 Mar 2010

Table 2. Example of results of statistical test suite Diehard for sequences generated using 6 LSBs. The sequence length is 74 Mbit. "KS" indicates that a single P-value is obtained by the Kolmogorov-Smirnov (KS) test [28]. For the tests which produce multiple P-values without the KS test, the worst case is shown.

STATISTICAL TEST	P-VALUE	RESULT	
birthsay spacing	0.882291	SUCCESS	KS
overlapping 5-permutaion	0.483639	SUCCESS	
binary rank for 31 × 31 matrices	0.658636	SUCCESS	
binary rank for 32 × 32 matrices	0.391334	SUCCESS	
binary rank for 8 × 8 matrices	0.367852	SUCCESS	KS
bitstream	0.056500	SUCCESS	
overlapping-Paris-Spares-Occupancy	0.000700	SUCCESS	
overlapping-Quardruples-Spares-Occupancy	0.015800	SUCCESS	
DNA	0.015800	SUCCESS	
count-the-1's on a stream of bytes	0.049820	SUCCESS	
count-the-1's for specific bytes	0.353940	SUCCESS	
parkihng lot	0.260828	SUCCESS	KS
minimum distance	0.326556	SUCCESS	KS
3D spheres	0.059882	SUCCESS	KS
speeze	0.458916	SUCCESS	
overlapping sums	0.965410	SUCCESS	KS
runs	0.181109	SUCCESS	KS
craps	0.812245	SUCCESS	
Total		18	

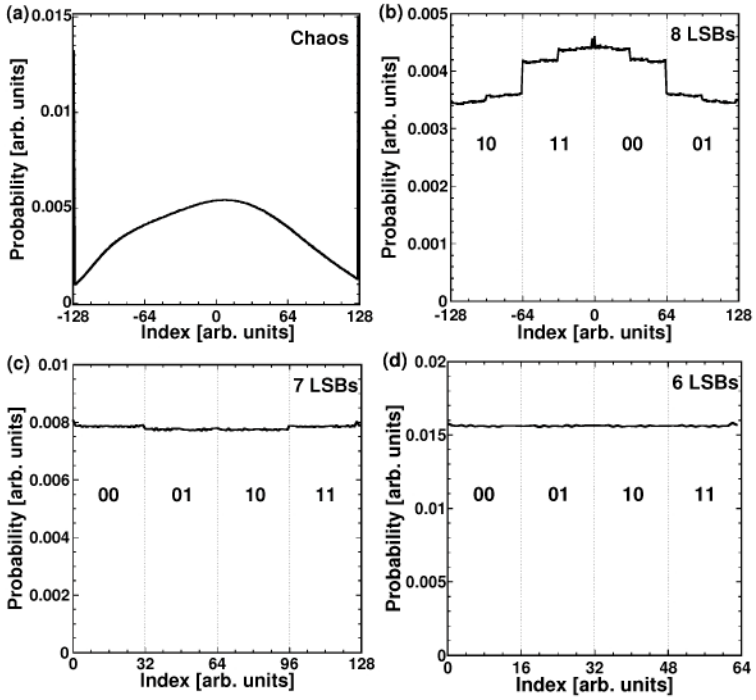

Fig. 5. Probability density functions for (a) 8-bit digitized chaotic waveform, (b) 8-bit random bits after bitwise XOR operation is applied to the two 8-bit digitized chaotic waveforms, (c) 7 LSBs selected from the 8-bit XOR data, and (d) 6 LSBs selected from the 8-bit XOR data.

The use of optical fiber components ensured stable oscillation conditions. Both the chaotic oscillations and sampling operations were stable with respect to mechanical and thermal

#121087 - $15.00 USD Received 7 Dec 2009; revised 12 Feb 2010; accepted 14 Feb 2010; published 3 Mar 2010

perturbations, to the extent that statistical properties of the sequences were maintained over hours of continual operation.

4. Statistical characteristics of random bits

In this section we present details of the randomness tests, showing the dependence of the randomness on the bits selected to create the sequences

4.1 Probability density function

First we investigate the probability density function of multi-bit states obtained from various LSBs. Figure 5(a) shows the distribution for 8-bit samples from one chaotic waveform. Figure 5(b) shows the distribution of 8-bit XOR samples after bitwise XOR of 8-bit samples from a chaotic waveform and the delayed waveform. The distribution becomes more uniform, but there are some discontinuities in the distribution of Fig. 5(b). When only 7 LSBs of the 8-bit XOR data are selected (Fig. 5(c)), the distribution becomes flatter. In the case of 6 LSBs of the 8-bit XOR data (Fig. 5(d)), the distribution appears almost uniform. The two-bit labels shown in Figs. 5(b)-5(d) indicate the first two most significant bits (MSBs) of the data generated from *m* LSBs (see Sec. 4.2).

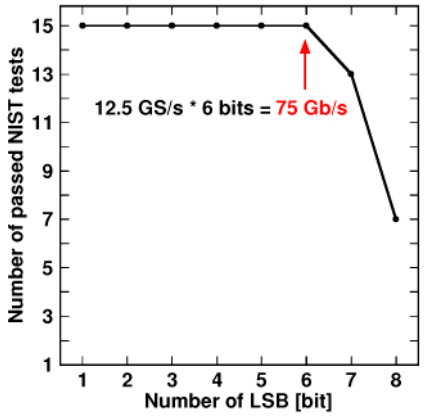

Fig. 6. The number of passed NIST SP 800-22 tests as a function of the number of least significant bits (LSBs) used to generate the bit sequence. “15” indicates that all the tests are passed.

4.2 NIST tests of sequences generated using multiple significant bits

Next, we investigate the dependence of the randomness test performance on the number of LSBs used. In particular, we show that up to 6 LSBs can be combined to create sequences which pass the tests of randomness.

Figure 6 shows the number of passed NIST SP 800-22 tests as a function of the number of LSBs. The number of LSBs is increased from “1”, corresponding to just the LSB, to “8” corresponding to all bits including the MSB. All the 15 tests are passed when the number of LSBs is set to a value between 1 and 6. In the case of 7 LSBs, only 13 tests are passed and the two tests of “runs” and “block-frequency” are failed. For 8 LSBs, only 7 tests are passed. The maximum length of LSBs used for random bits that pass all the NIST tests is 6 LSBs. This result is consistent with the uniformity of the probability density functions shown in Fig. 5(d). The use of 6 LSBs obtained at the sampling rate of 12.5 GS/s corresponds to the generation rate of 75 Gb/s.

To give more insight into the dependence on the number of LSBs used, we focus on two tests in NIST SP 800-22: runs and block-frequency tests, which are failed when too many LSBs are used. The runs test examines the occurrence of uninterrupted sequences of identical bits, and the block-frequency test investigates the frequency of “1” (i.e., 0/1 ratio) within a specified block length. Figure 7(a) shows the results of the runs and block-frequency tests in

#121087 - $15.00 USD Received 7 Dec 2009; revised 12 Feb 2010; accepted 14 Feb 2010; published 3 Mar 2010

NIST SP 800-22 for sequences generated using various numbers of LSBs. The uniformity of p-values (referred to as P-value in Table 1) is plotted as a function of the number of LSBs used. The P-value needs to be larger than 10^{-4} to pass the test. The P-value gradually decreases as the number of LSBs increases. Both the runs and block-frequency tests are passed when the length of LSBs is set to be up to 6 LSBs.

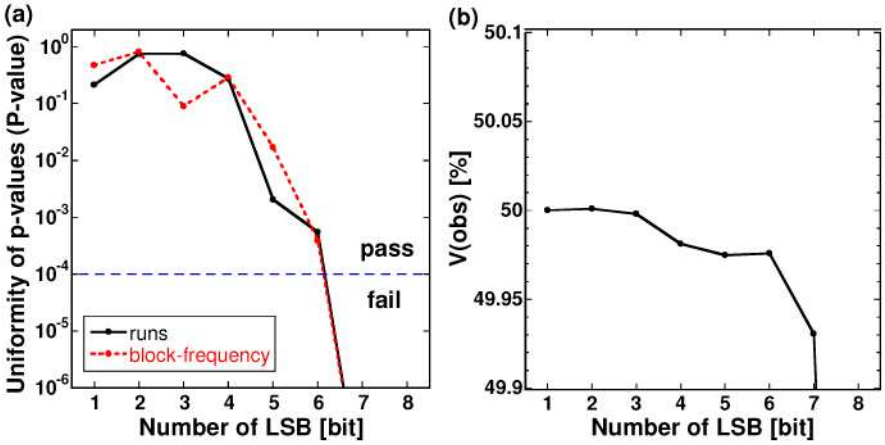

Fig. 7. Statistical test measures as a function of the number of least significant bits (LSBs) used to generate the bit sequence. (a) Uniformity of p-values (referred to as P-value in Table 1) for the runs test (black solid curve) and block-frequency test (red dotted curve) in NIST SP 800-22 and (b) Ratio of V(obs) as a function of the number of LSBs. (a) P-value needs to be larger than 10^{-4} to pass the test criteria (blue dashed line). The P-values for 7 and 8 LSBs are 0 (out of range in the figure). The block length is 128 bit for the block-frequency test. (b) *V(obs)* for 8 LSBs is 49.328% (out of range in the figure).

The runs test examines the frequency of occurrence of uninterrupted sequences of identical bits. The ratio of runs *V(obs)* is calculated as follows [26].

$$V(obs) = \frac{1}{n}\left[\left\{\sum_{k=1}^{n-1} r(k)\right\} + 1\right] \times 100\,[\%] \tag{1}$$

$$r(k) = \begin{cases} 0 & \varepsilon_k = \varepsilon_{k+1} \\ 1 & \varepsilon_k \neq \varepsilon_{k+1} \end{cases} \tag{2}$$

where n is the length of the bit string, ε the sequence of bits being tested ($\varepsilon = \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$; $\varepsilon_k = 0$ *or* 1). As seen in Eq. (1) and Eq. (2), *V(obs)* is the ratio of the number of occurrences of two inverted consecutive bits ("01" or "10") in the whole bit sequence. Note that *V(obs)* in Eq. (1) indicates the ratio of runs, whereas *V(obs)* is defined as the number of runs in NIST SP 800-22 [26]. Figure 7(b) shows *V(obs)* computed over the total sequence data of 1 Gigabit (= 1 Megabit × 1000 samples), plotted as a function of the number of LSBs. We found that *V(obs)* is close to the ideal average value of 50% for 1, 2 and 3 LSBs, starts to deviate for 4, 5, and 6 LSBs, and deviates significantly for 7 and 8 LSBs. This deviation of the *V(obs)* is related to the non-uniformity of the probability density functions shown in Fig. 5(b) and 5(c), where the first two MSBs corresponding to identical bits ("00" or "11") has more probability than that for the inverted bits ("01" or "10"). Here we have considered one particular method of ordering multiple LSBs to create a single sequence as shown in Fig. 3. It is possible that the performance of the runs test might be improved by using different ordering.

#121087 - $15.00 USD Received 7 Dec 2009; revised 12 Feb 2010; accepted 14 Feb 2010; published 3 Mar 2010

4.3 NIST tests of sequences generated using single significant bits

Next we investigate the randomness of sequences generated using only one of the 8-bits acquired at each sample time. In particular, we show that each of the 7 LSBs (i.e., excluding the MSB) passed the statistical tests of randomness. This is consistent with the above results for sequences created using multiple significant bits, considering that there may be some correlations between bits which affect statistical properties when more than one significant bit is used.

Figure 8 shows the number of passed NIST SP 800-22 tests as a function of the significant bit used for generating random bits. All the 15 tests are passed by sequences generated using the significant bits 1 to 7. When the significant bit 8 (i.e., MSB) is used, only 6 tests are passed.

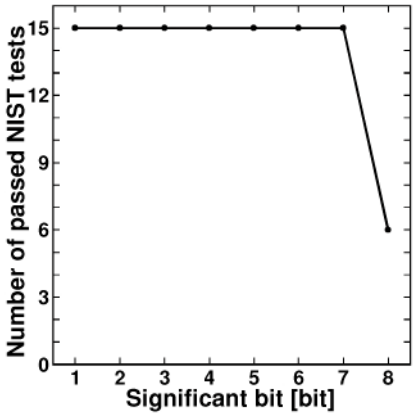

Fig. 8. The number of passed NIST SP 800-22 tests as a function of the significant bit. (Significant bit 1 is LSB; significant bit 8 is MSB.) The sequences are generated using only one of the 8 bits acquired at each sample time. "15" indicates that all the tests are passed.

Figure 9(a) shows the test results of the runs and block-frequency tests in NIST SP 800-22 for the random bit sequences generated using one significant bit. The uniformity of p-values (P-value) is plotted as a function of the significant bit. The P-value stays high between 10^{-1} and 10^{0} for the significant bits 1 to 7. Both the runs and block-frequency tests are passed by all significant bits up to 7. Figure 9(b) shows *V(obs)* as a function of the significant bit. *V(obs)* is close to 50% for the significant bits 1 to 7, and decreases significantly for the significant bit 8 (i.e., MSB). The 0/1 ratio of the MSB is more sensitively dependent on the match between the signal amplitudes and the range of the 8-bit detectors, compared with the other bits. We do not exclude the possibility of improving the test performance of MSB sequences by adjusting the signal offset or amplitude with respect to the MSB detection threshold [11,13].

Very recently, Kanter and associates have reported that bit sequences passing the NIST tests can be generated at higher bit rates up to 300 Gb/s using a single chaotic semiconductor laser by retaining a number of the LSBs of the value of a high derivative of the digitized chaotic laser intensity [29]. However, the bandwidth of the laser chaos is only a few GHz in their scheme. This suggests that the reported bit rate exceeds the capacity of the laser chaos to generate non-deterministic random bits. Moreover, extracting more bits from high derivatives could be more susceptible to the effects of physical noise in the AD converter - a potential additional source of randomness which is separate from the laser chaos. A strong motivation for using direct sampling of optical chaos for random number generation is to reduce the dependence on digital electronic operations, which may be difficult to implement at high frequencies, and which in principle cannot increase the rate for generation of non-deterministic bits. From these points of view, it is very important to increases the bandwidth of the laser chaos used for random number generation.

#121087 - $15.00 USD Received 7 Dec 2009; revised 12 Feb 2010; accepted 14 Feb 2010; published 3 Mar 2010

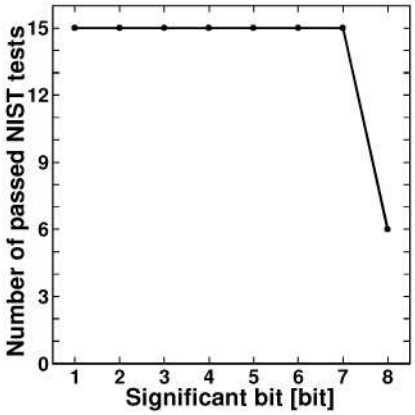

Figure 8 The number of passed NIST SP 800-22 tests as a function of the significant bit. (Significant bit 1 is LSB; significant bit 8 is MSB.) The sequences are generated using only one of the 8 bits acquired at each sample time. "15" indicates that all the tests are passed.

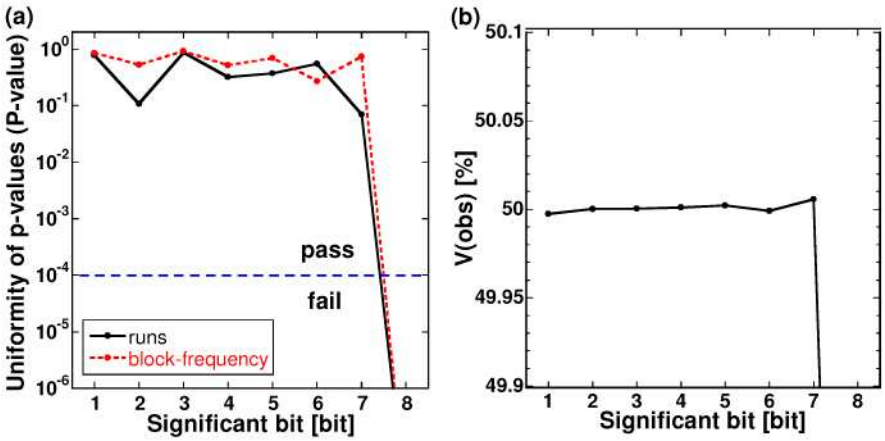

Fig. 9. Statistical test measures as a function of the significant bit. (Significant bit 1 is LSB; significant bit 8 is MSB.) (a) Uniformity of p-values (referred to as P-value in Table 1) for the runs test (black solid curve) and block-frequency test (red dotted curve) in NIST SP 800-22 and (b) Ratio of *V(obs)* as a function of the significant bit. (a) P-value needs to be larger than 10^{-4} to pass the test criteria (blue dashed line).

5. Conclusion

We have experimentally demonstrated a method for physical random bit generation using bandwidth-enhanced chaos in semiconductor lasers. Bandwidth-enhanced chaos is realized by taking the chaotic light from a semiconductor laser with optical feedback and injecting it into a second semiconductor laser. We have used this technique to realize chaotic laser signals with bandwidth enhanced up to 16 GHz. The use of this bandwidth enhanced chaos allows us to generate random bits by sampling the chaotic signal at the high rate of 12.5 GS/s. In the experiment, we used a high-speed digital oscilloscope to record 8-bit samples at 12.5 GS/s simultaneously on two channels from a chaotic laser signal and its time-delayed signal. Random bits are then obtained by bitwise XOR operation on corresponding bits of the two digital signals. 7 of the 8 significant bits (i.e., all bits except MSB) obtained separately by the oscilloscope passed statistical tests of randomness. Moreover, sequences obtained by interleaving up to 6 LSBs also passed the statistical tests of randomness. These results correspond to random bit generation rates from 12.5 to 75 Gb/s (= 6 bit × 12.5 GS/s).

#121087 - $15.00 USD Received 7 Dec 2009; revised 12 Feb 2010; accepted 14 Feb 2010; published 3 Mar 2010

Acknowledgments

We thank Yoshinobu Tonomura, Naonori Ueda, Kenji Nakazawa, and Atsushi Nakamura for their support and encouragement. We thank Ido Kanter, Laurent Larger, Junji Ohtsubo, and Dimitris Syvridis for helpful discussions and comments. We acknowledge support from TEPCO Research Foundation, The Mazda Foundation, and Grant-in-Aid for Young Scientists from the Ministry of Education, Culture, Sports, Science and Technology in Japan.

#121087 - $15.00 USD Received 7 Dec 2009; revised 12 Feb 2010; accepted 14 Feb 2010; published 3 Mar 2010