Incoherent fibre supercontinuum generation for all-optical random number generation

B. Wetzel[1], L. Larger[1], K. J. Blow[2], S. K. Turitsyn[2], J. M. Dudley[1]

[1]*Institut FEMTO-ST, UMR 6174 CNRS- Université de Franche-Comté, 25030 Besançon, France*

[2]*Photonics Research Group, Electronic Engineering, Aston University Birmingham, England*

Random number generation is a central component of modern information technology, with crucial applications in ensuring communications and information security. The development of new physical mechanisms suitable to directly generate random bit sequences is thus a subject of intense current research, with particular interest in all-optical techniques suitable for the generation of data sequences with high bit rate. One such promising technique that has received much recent attention is the chaotic semiconductor laser systems producing high quality random output as a result of the intrinsic nonlinear dynamics of its architecture [1]. Here we propose a novel complementary concept of all-optical technique that might dramatically increase the generation rate of random bits by using simultaneously multiple spectral channels with uncorrelated signals - somewhat similar to use of wave-division-multiplexing in communications. We propose to exploit the intrinsic nonlinear dynamics of extreme spectral broadening and supercontinuum (SC) generation in optical fibre, a process known to be often associated with non-deterministic fluctuations [2]. In this paper, we report proof-of concept results indicating that the fluctuations in highly nonlinear fibre SC generation can potentially be used for random number generation.

The noise and coherence properties of fibre SC generation are well-known to depend on the precise choice of source and fibre parameters [2]. In physical terms, when the input pulse duration is in the sub-100 fs regime, the low intensity wings of the pulse spectrum extends into the typical wavelength range where modulation instability (MI) gain is observed. The presence of a coherent spectral seed in this wavelength region ensures that spontaneously-generated spectral content from noise-seeded MI has negligible influence on the SC dynamics and thus a coherent SC spectrum results. On the other hand, for longer pulse durations, there is progressive destabilisation of the SC stability as the pump bandwidth is reduced, such that the spontaneous generation from noise of spectral components competes with broadening mechanisms coherent with the pump. For picosecond and nanosecond pulses, this yields highly unstable incoherent SC spectra. The statistics of such incoherent spectra have recently been studied in the context of ``optical rogue wave'' fluctuations associated with the appearance of rare large amplitude events on the long wavelength edge of the spectrum. However, it has been shown that such statistics depend sensitively on the particular wavelengths studied in the spectrum, and we have used this fact to develop a procedure for random number generation associated with selecting particular wavelength ranges in the spectrum where the statistics is normally distributed about some mean value.

The approach is illustrated in the figure below where we outline the proposed principle using an ensemble of 1000 simulations. Fig. 1(a) shows an ensemble of spectra associated with incoherent SC generation [3] whilst Fig. 1(b) shows the peak power time series from filtering over 1700-1900 nm and extracting the corresponding temporal signal; this time series is well-fitted by a Gaussian distribution. To use this data for random number generation, we calculate a rolling median across the time-series and find that this stabilises after typically 1000 events; this median then establishes a threshold dividing the time series into bits 1 and 0 above and below the median. We use this threshold from the first 1000 records to create a bit sequence over subsequent records for a much longer sequence length (~10^5). The resulting bit sequence satisfies standard tests as well as classical pseudo random distributions based on National Institute of Science and Technology (NIST) benchmark test suite. Details of the proposed novel all-optical technique based on application of non-coherent SC as possible random number generator will be presented at the conference.

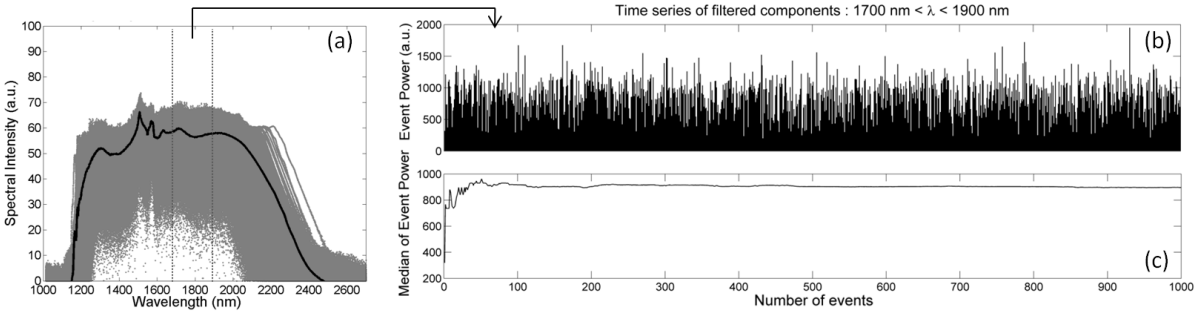

Fig. 1 Incoherent SC generation; grey curves show individual realizations; black shows the mean. (b) Time series of temporal power with 1700-1900 nm filtering. (c) Evolution of the rolling median showing that the time series can be associated with a threshold for the definition of bits that generate a random sequence.

References

[1] A. Uchida *et al.* Nature Photonics **2**, 728-732 (2008) ; I. Kanter *et al.* Nature Photonics **4**, 58 - 61 (2010)

[2] J. M. Dudley *et al.* Rev. Mod. Phys. **78** 1135-1184 (2006); S. V. Smirnov *et al.* Opt. Fiber Technol. 12, 122-147 (2006)

[3] Here we use parameters: 3 ps pulse injected in 15m photonic crystal fiber with 400 W peak power at λ= 1550 nm, very close to ZDW (β_2= 1.3.10^{-1} $ps^2.Km^{-1}$, β_3= 6.48.10^{-2}, γ= 0.01066 $W^{-1}.m^{-1}$)