Highly parallel ultra-fast random number generation from a stable-cavity broad-area semiconductor laser

Kyungduk Kim, S. Bittner, Yongquan Zeng, Stefano Guazzotti, Ortwin Hess, Qi Jie Wang, Hui Cao

Highly parallel ultra-fast random number generation from a stable-cavity broad-area semiconductor laser

Kyungduk Kim[1], Stefan Bittner[1,2], Yongquan Zeng[3], Stefano Guazzotti[4], Ortwin Hess[4], Qi Jie Wang[3], Hui Cao[1]

1. Department of Applied Physics, Yale University, 15 prospect street, CT 06511 New Haven, USA
2. Chair in Photonics, LMOPS EA-4423 Laboratory, CentraleSupélec and Université de Lorraine, 2 rue Edouard Belin, Metz 57070, France
3. Center for OptoElectronics and Biophotonics, Nanyang Technological University, 50 Nanyang Avenue, 639798 Singapore
4. School of Physics and CRANN Institute, Trinity College Dublin, Dublin 2, Ireland

Fast and reliable random number generation (RNG) is a key requirement for, e.g., secure telecommunication or quantum simulations. This has driven the development of physical random number generators to replace deterministic, pseudo-random number generators. Semiconductor lasers exhibiting chaotic dynamics induced for example by optical feedback [1] can provide up to 1 Tbit/s, but their speed is ultimately limited by the time scales of the laser dynamics. Parallel RNG via spatial or spectral multiplexing can further increase the speed but previous demonstrations were limited by low intrinsic speed or a small number of channels.

Broad-area semiconductor lasers (BALs) exhibit fast dynamics in a high number of spatial channels. However, conventional Fabry-Perot BALs suffer from filamentation that induces spatio-temporal correlations which prohibit the generation of uncorrelated random bit streams [2]. We developed an on-chip stable-cavity laser with curved facets [Fig. 1(a)] exhibiting hundreds of transverse modes [2]. The resulting complex many-mode interference suppresses the filamentation [3], and the laser emits a spatio-temporal speckle pattern that we measured with picosecond time resolution using a streak camera [Fig. 1(b)]. The spatio-temporal correlation function [Fig. 1(c)] shows a correlation time of the order of a picosecond determined by the inverse of the width of the laser spectrum instead of the time scales of a chaotic laser dynamics. Moreover, there are no long-range spatio-temporal correlations.

In a proof-of-principle experiment we demonstrate ultra-fast, highly parallel random number generation by offline post-processing with the laser shown in Fig. 1(a). In total 127 bit streams are extracted from the spatio-temporal measurements by our digitization procedure using the 3 least-significant bits out of 6 bits. With a rate of 2 Tbit/s per stream, we thus obtain a total rate of about 250 Tbit/s which is two orders of magnitude faster than the current record for post-processing. The randomness as well as independence of the different bit streams was confirmed with standard random number test suites.

In conclusion, we present a new paradigm for RNG based on complex multi-mode interference in a broad-area stable-cavity semiconductor laser. Our RNG scheme allows both higher single-channel bit rates as well as more parallel bit streams than previous approaches. Since the spontaneous emission (i.e., quantum fluctuations) constantly feeds noise into the lasing modes, their interference pattern is unpredictable and the resulting bit streams are truly random. Moreover, the laser device is compact, robust, and no fine tuning of the operation parameters is needed. However, significant technological development will be necessary to create an integrated random number generator for real-world applications.

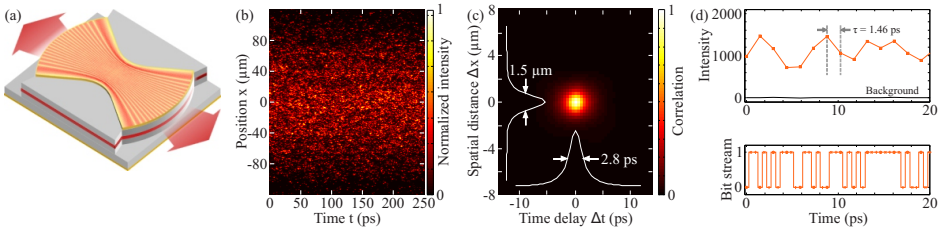

Fig. 1 (a) Schematic of edge-emitting on-chip stable-cavity semiconductor laser (800 μm long and 566 μm wide). (b) Spatio-temporal speckle pattern of laser emission measured by a streak camera. (c) Spatio-temporal correlation function of laser emission. (d) Intensity time trace from a single spatial channel sampled at 1.46 ps (top) and the resulting random bit stream with 3 bits per sample (bottom).

References

[1] 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," Nature Photonics **2**, 728 (2008).
[2] K. Kim, S. Bittner, Y. Zeng, S. Guazzotti, O. Hess, and H. Cao, "Massively parallel ultrafast random bit generation with a chip-scale laser," arXiv:2004.07157 (2020).
[3] S. Bittner, S. Guazzotti, Y. Zeng, X. Hu, H. Yılmaz, K. Kim, S. S. Oh, Q. J. Wang, O. Hess, and H. Cao, "Suppressing spatio-temporal lasing instabilities with wave-chaotic microcavities," Science **361**, 1225 (2018).