Massively Parallel Random Numbers with a Laser Diode

As we rely more and more on digital networks, rapidly generating large numbers of high-quality random numbers is becoming urgent for cybersecurity. At present, random numbers are usually "pseudo-random," being generated by deterministic algorithms. They thus leave information security and cryptography applications vulnerable to attack, and can produce inaccurate or erroneous results in other applications such as stochastic modeling and quantum simulations.

True random numbers, needed for such sensitive applications, are generated by sampling real physical phenomena—but in most cases the generation rate is low and the cost is high. Semiconductor lasers with chaotic dynamics have been employed for high-speed random-bit generation (RBG).[1] While the bit generation rate has been boosted to terabits per second, the intrinsic timescales of the chaotic dynamics ultimately limit the generation rate. We recently explored a different physical process with much faster dynamics to greatly enhance the RBG rate in a single channel, and achieved parallel RBG with hundreds of spatial channels in a broad-area laser diode.[2]

The first step toward parallel RBG with a broad-area semiconductor laser is suppressing its spatio-temporal instabilities, which introduce long-range spatial and temporal correlations of the emission intensity that degrade the quality of random bitstreams. We used a simple yet effective method to suppress lasing instabilities: tailoring the cavity geometry by curving the end facets, which enhances lateral optical confinement and dramatically increases the number of transverse lasing modes.[3] The high-order transverse modes create small-scale intensity variations that effectively prevent filamentation and instabilities and greatly shorten the spatio-temporal correlation lengths.[4]

Once the lasing instability is suppressed, spatio-temporal interference of hundreds of transverse and longitudinal lasing modes creates a complex emission pattern. The ultrashort correlation scales—1.5 μm in space and 2.8 ps in time—enable ultrafast parallel random bit generation via spatial multiplexing.[2] Spontaneous emission adds stochastic noise to render the intensity fluctuations unpredictable and non-reproducible.

With offline post-processing, we were able to generate 127 independent bitstreams simultaneously, with a bit rate of 2 Tbit/s per stream. The total bit rate reached 254 Tbit/s, two orders of magnitude above the current record with post-processing—and standard statistical test suites verified the high quality of the random bits. Our approach is robust, compact and energy efficient, and should impact applications in secure communications and high-performance computation. OPN

RESEARCHERS

Kyungduk Kim and **Hui Cao** (hui.cao@yale.edu), Yale University, CT, USA

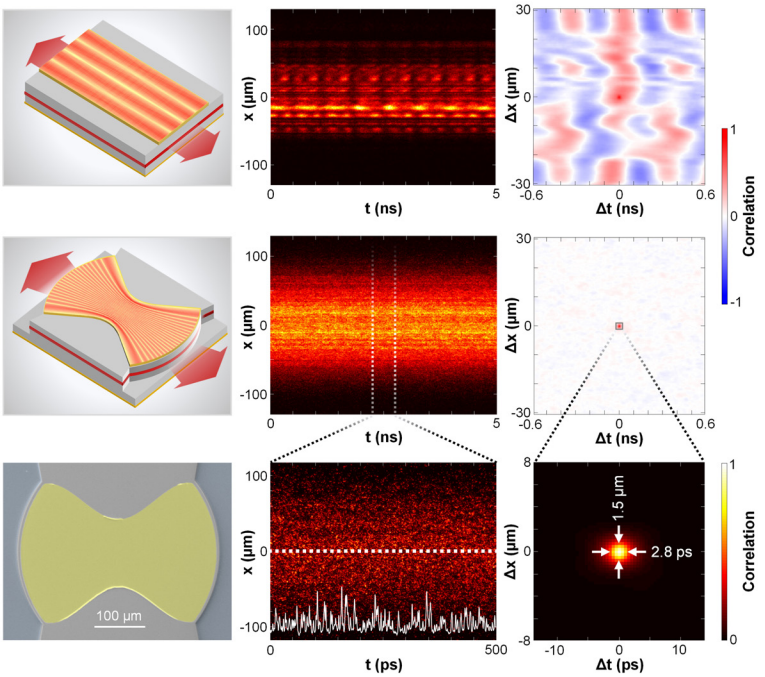
Stefan Bittner, CentraleSupélec, France

Yongquan Zeng and **Qi Jie Wang**, Nanyang Technological University, Singapore

Stefano Guazzotti and **Ortwin Hess**, Trinity College Dublin, Ireland

REFERENCES

1. J.D. Hart et al. APL Photon. **2**, 090901 (2017).
2. K. Kim et al. Science **371**, 948 (2021).
3. K. Kim et al. Appl. Phys. Lett. **115**, 071101 (2019).
4. S. Bittner et al. Science **361**, 1225 (2018).



In contrast to a wide-stripe edge-emitting semiconductor laser with planar facets (top row), a laser with both end facets curved (middle row) suppresses lasing instabilities and eliminates long-range intensity correlations that can compromise random-bit generation (RBG). Bottom row: A fabricated laser diode supports many lasing modes whose interference creates ultrafast spatio-temporal intensity fluctuations used for parallel RBG.

K. Kim et al. Science **371**, 948 (2021)