Random Number Generation Using Amplified Spontaneous Emission in a Fiber Amplifier

Julia C. Salevan, Caitlin Williams, Xiaowen Li, Thomas E. Murphy, Rajarshi Roy

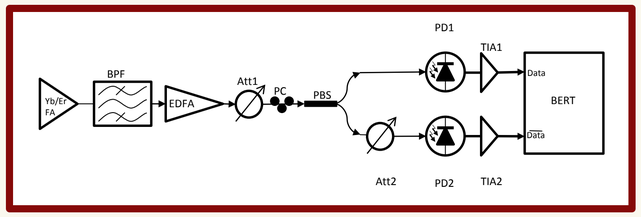
University of Maryland 18 56 — TREND FAIR 2010

Institute for Research in Electronics & Applied Physics

Introduction

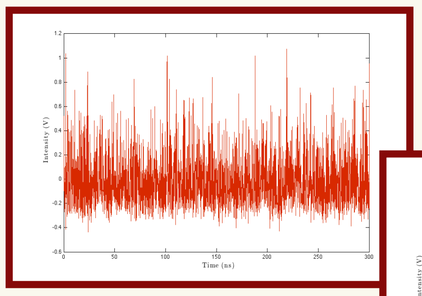
- Random number generators (RNGs) have wide-ranging applications including cryptography and Monte Carlo simulations, some of which require high-speed random number generation.
- Computer-based pseudo-random number generators (PRNGs) can generate numbers at high speeds, but are necessarily deterministic.
- Recent high-speed, physical, true random number generators have used optical methods including photon counting and chaotic systems.
- We examine an optical system using the amplified spontaneous emission in a fiber amplifier as our random source.

System

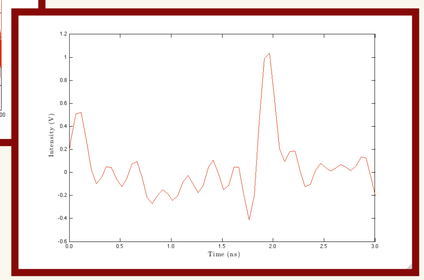


Yb/Er FA: Ytterbium/Erbium Fiber Amplifier — BPF: Band Pass Filter
EDFA: Erbium Doped Fiber Amplifier — Att: Attenuator
PC: Polarization Controller — PBS: Polarizing Beam Splitter
PD: Photodetector — TIA: Trans Impedance Amplifier
BERT: Bit Error Rate Tester

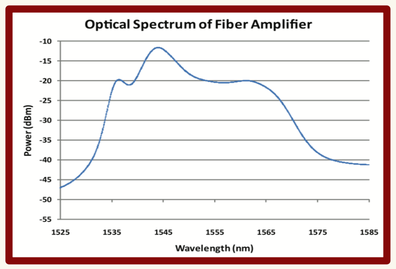
- Filter and amplify high-bandwidth noise in a fiber amplifier
- Split the beam and attenuate to balance the two signals
- Bit Error Rate Tester subtracts the two signals, samples at 12.5 GHz to convert to bits

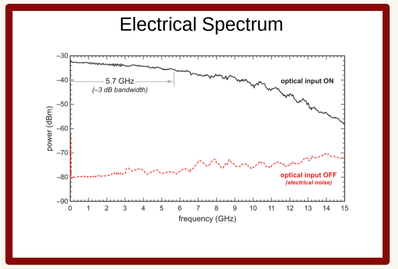


Time trace, 300ns length



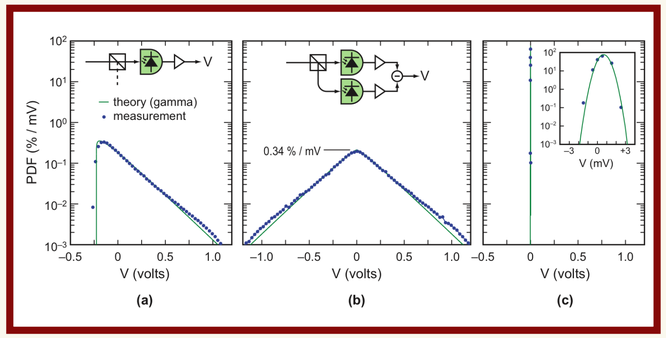
Time trace detail, 3ns





Balancing

- Asymmetric voltage distribution has different mean and median, so threshold changes as power fluctuates
- Two detectors used to symmetrize signal about zero
- Automated program written to measure statistics

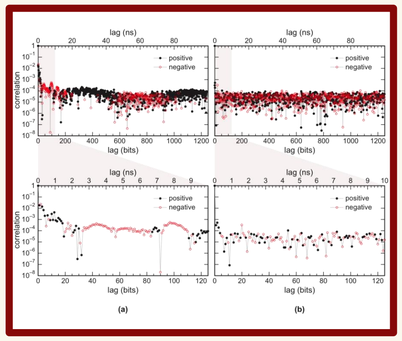


Statistical Testing

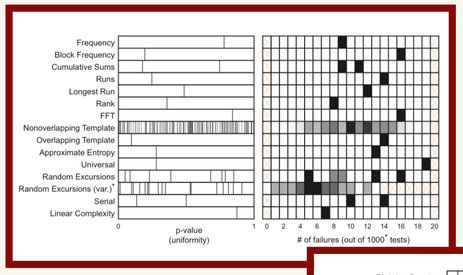
- The NIST Statistical Test Suite consists of 15 tests for specific types of nonrandomness.
- It is the only test suite available for testing both PRNGs and physical RNGs.
- To pass the tests, the P-value (uniformity of p-values) must be greater than 0.0001, and out of 1000 tests, must be fewer than 20 failures
- The DIEHARD tests are an older suite of 18 tests developed for PRNGs that, along with the NIST STS, are accepted as industry standard to test for nonrandomness
- NIST STS requires 1000 1Mbit samples, DIEHARD requires one 74 Mbit sample

Results

- At 12.5 Gbits/s, the raw data displays high autocorrelations at small lags, and oscillating patterns in the autocorrelation across longer lags (a).
- We take the XOR between the data and a shifted duplicate of itself to reduce correlation and bias.
- The autocorrelation of the resultant bitstream (b) quickly drops below the noise floor and displays no obvious pattern.

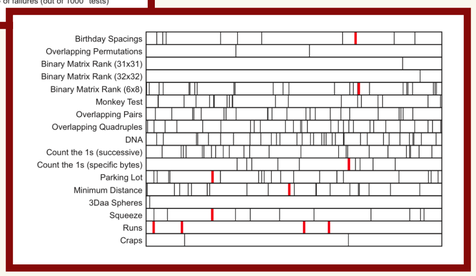


Resultant bitstream passes all NIST and DIEHARD tests.



NIST test P-values and # of failures

DIEHARD test p-values



Conclusions and Future Work

- We demonstrate a high-speed, physical random number generator that can be implemented entirely in hardware.
- Success in statistical testing shows that our system meets industry standards for cryptographic security.

Future Work

- Automate data acquisition
- Consider LED or other incoherent sources
- Improve shielding from electromagnetic and other interference
- Scale system to multiple wavelengths