FiO LS
Frontiers in Optics + Laser Science
Presentation No: JTu5A.57

Femtosecond Laser based Post-Processing Free True Random Number Generator

Amritash Sharma[1, 3, †], Prasanna Paithankar[1, 2, †] and Shailendra K. Varshney[1]

[1]Fiber Optics, Nano and Quantum Photonics (FONQP) Group, Advanced Photonics Laboratory, Department of Electronics and Electrical Communication Engineering,
[2]Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur, West Bengal 721302, India
[3]Department of Applied Optics and Photonics, University of Calcutta, Technology Campus, JD 2, Salt Lake, Kolkata 700098, India
[†]Authors contributed equally

Abstract

We experimentally demonstrate a high-entropy source based on the intensity fluctuation in a femtosecond laser. The setup successfully passes statistical tests without any post-processing. The true generator can be potentially used for quantum key distribution and photonic computation.

Optical Setup

- The device setup consists of a Ytterbium doped duct pulse amplification based mode locked fiber laser - ORPHEUS-Carbide femtosecond laser, a beam splitter, followed by a Si photodiode. The silicon photodiode has a maximum receptivity at 810 nm.
- The source of randomness originates from the laser source (femstosecond laser), where the working parameters of the laser are : 810 nm wavelength, 500.7 kHz repetition rate, 120 mW average operational power and an energy split ratio of 1:60.
- The resistance accompanying the photodiode must be calibrated to achieve safe and reasonable voltage values to the analog to digital converter (ADC).

Introduction

- Algorithm-based PRNGs, although refined, cannot provide the physical randomness necessary for applications like quantum cryptography, where unpredictable bit strings are essential to ensure the inability of estimation (Shannon's maxim).
- In this model the TRNG is based off of thermal fluctuations in the Chirped Pulsed Amplification based fiber pump laser sampled at a high rate.
- The raw output is ready to be used as a cryptographically secure random number stream as benchmarked.
- The min-entropy of the source of about 6.55 bits which surpasses previously reported RNG's in literature.

Data Acquisition

- The intensity output data from the APD is continually fed to an n-bit ADC. The digital data is further sent into an analog memory block (n s-bit SIPO shift registers).
- At every clock cycle, the last data and first memory address are subtracted. The LSB bit of the readout is considered for output.
- The limiting factor affecting the output stream bit rate is the sampling rate (maximum APD sampling rate is taken into consideration in GHz range).

Statistical Test	P-value	Result
Frequency	0.0043	Pass
Block Frequency	0.7399	Pass
Cumulative Sums	0.5341	Pass
Longest Run	0.5341	Pass
FFT	0.5341	Pass
Non Overlapping Template	0.7399	Pass
Overlapping Template	0.3504	Pass
Approximate Entropy	0.5341	Pass
Serial	0.9114	Pass
Linear Complexity	0.3505	Pass
Universal	------	Pass
Random Excursions	------	Pass

Table 1. Result of NIST Statistical Randomness Test Suite. P-value = 0.0001 passes a given test.

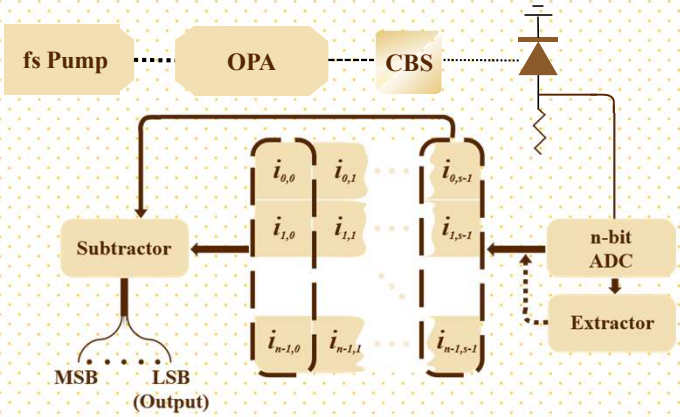

Figure 1. The RNG consisting of the Optical setup comprising of the fs laser source, OPA and a beam splitter whose beam is shined upon a Si photodiode. The data processor packs a digitizer and a register bank to stream raw bits through delayed difference. An optional conditioner can be used as an extractor.

Statistical Benchmarking

- Raw data-streams have successfully passed all NIST STS and Dieharder Tests with significant P-values.
- Ready to be employed in most critical cryptographic systems.
- Raw stream can be fed into extractors and psesudorandom generators to boost bitrate for less sensitive applications.

Scan the QR to view all results.

Bounding and Min-Entropy

- Given the experimental setup, the upper bound of extractable entropy is calculated to be

$$\max \mathrm{H}_S(X) = 57.76 \text{ bits}$$

of which we extract 10 bits.

- The min-entropy measure which quantifies randomness

$$\mathrm{H}_\infty(X) = \min_{x \in \mathrm{Supp}(X)} (-\log \Pr[X = x]) \geq 6.55 \text{ bits}$$

which surpasses previously reported TRNG values.

Conclusion

We have experimentally demonstrated a novel True Random Number Generator with a high bit-rate which is only limited by the device I/O and clock speed. The output streams have passed all stringent statistical tests. The technology can be readily used in domains of quantum communication, cryptography & computation

References

[1] J. F. Dynes, , et al., "A high speed, postprocessing free, quantum random number generator." Appl. Phys. Lett. 93 (3): 031109, (2008)
[2] Wei Wei and Hong Guo, "Bias-free true random-number generator," Opt. Lett. 34, 1876-1878 (2009)
[3] B. K. Park et al., "Practical True Random Number Generator Using CMOS Image Sensor Dark Noise," in IEEE Access, vol. 7, (2019)