Femtosecond Laser based Post-Processing Free True Random Number Generator

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

[1] *Fiber Optics, Nano and Quantum Photonics (FONQP) Group, Advanced Photonics Laboratory, Department of Electronics and Electrical Communication Engineering, Indian Institute of Technology Kharagpur, West Bengal 721302, India*

[2] *Department of Applied Optics and Photonics, University of Calcutta, Technology Campus, JD 2, Salt Lake, Kolkata 700098, India*

[3] *Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur, West Bengal 721302, India*

[†] *Authors contributed equally*

[*] *skvarshney@ece.iitkgp.ac.in*

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 generator can be potentially used for quantum communication and cryptography.

1. Introduction

Random number generators (RNGs) play a crucial role in various scientific, technological, and cryptographic applications, providing a fundamental source of entropy essential for generating uniform or non-uniform independent and identically distributed (i.i.d.) outcomes. Despite significant advancements in pseudorandom-number generators (PRNGs), with improved generation rates and robustness against benchmarking tests, they still suffer from a fundamental limitation: the eavesdropper can predict the next bit with a probability > 50, given Shannon's maxim. 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. True random-number generators (TRNGs) utilize physical random phenomena, such as the decay of radioactive nuclei, thermal noise in resistors, frequency jitter of electronic oscillators, and photon emission noise, as sources for generating nondeterministic random numbers [1–3]. TRNGs extract random bits from these physical processes, resulting in much higher entropy compared to algorithm-based pseudo-random-number generators. Specifically, in the case of photon emission noise, random bits are obtained either from the random time intervals between photon emissions of semiconductors or from the collapse of the photon wave function during random gating cycles. However, it is worth noting that the timing precision in these schemes poses a limitation on the rate at which random bits can be generated. Hereby, we propose a TRNG based on laser intensity variation caused by crystal oscillation and photon emission noises.

2. Experiment

2.1. 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, all operating at 20°C, 33% humidity and standard atmospheric pressure. The silicon photodiode has a maximum receptivity at 810 nm. The beamsplitter works as a constant reflectance attenuator, i.e. causing a constant reduction in energy without variance in intensity fluctuations. 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).

2.2. Online Processing

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 serial-in-parallel-out (SIPO) shift registers). At every clock cycle, the last data and first memory address are subtracted. The LSB bit of the absolute number is considered as the 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). Being a strong entropy source, data post-processing with application of randomness

extractors was not necessary. A common randomness extractor and conditioning component can be used to refine the stream at the cost of lower bit-rate [4].

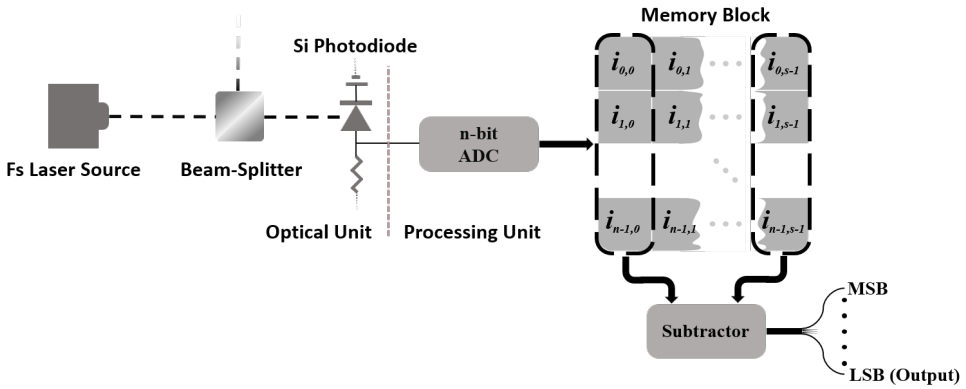

Fig. 1. Schematic outlining optical setup on the left and the computational units on the right.

3. Results

The data stream was collected in ASCII format and then benchmarked using NIST Statistical Test Suite and Dieharder tests [4]. The test results were highly satisfactory even without post-processing. The NIST STS results have been tabulated in Table 1.

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
Random Excursions Variant	- - - - -	Pass

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

The output rate is primarily influenced data channel baud rate, which is normally lower than the clock speed. We can easily attain 10^6 bits/s by setting the output and device baud rate to that value. To achieve in Giga-bit/s range, only the hardware I/O must be upgraded.

4. 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 and computation.

References

1. J. F. Dynes, Z. L. Yuan, A. W. Sharpe, A. J. Shields, "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, pp. 91407-91413, (2019)
4. Meltem Sönmez Turan, et al., "NIST Special Publication 800-90B: Recommendation for the Entropy Sources Used for Random Bit Generation," https://doi.org/10.6028/NIST.SP.800-90B (2018)