Quantum random number generator based on silicon nanocrystals LED

Zahra Bisadi[1,a], Alessio Meneghetti[2], Giorgio Fontana[1], Georg Pucker[3], Paolo Bettotti[1] and Lorenzo Pavesi[1]

[1]Nanoscience Laboratory, Department of Physics, University of Trento, Via Sommarive 14, Povo 38123, Italy
[2]Department of Mathematics, University of Trento, Via Sommarive 14, Povo 38123, Italy
[3]Center for Materials and Microsystems, FBK, Via Sommarive 18, Povo 38123, Italy
[a]zahra.bisadi@unitn.it

Abstract

We present a post-processing free quantum random number generator (QRNG) based on silicon nanocrystals (Si-NCs) LEDs as a source of randomness. The relatively simple setup for data extraction, a negligible bias measured from the datasets and applying no post-processing operations to the raw data are the main advantages of this QRNG . The obtained bit sequences pass all the NIST tests and the highest bit-rate achieved is 0.6 Mbps.

A. Introduction

Random numbers are highly significant in many applications including Monte Carlo simulations [1, 2] and particularly cryptography [3, 4] where producing unpredictable results is absolutely vital to guarantee complete security of data transmission. In several situations random numbers are obtained through pseudo random number generators (PRNG) which are deterministic algorithms able to output long sequences of bits at high bit-rates. However, their unpredictability is not totally assured since when the seed (initial value) is revealed, all the bits in the sequence will consequently be constructed. Contrary to pseudo random numbers, truly random numbers essentially need to be generated through physical nondeterministic processes [3]. These processes include a wide range of physical phenomena fundamentally based on quantum physics. The main disadvantage of physical RNGs is the difficulty of obtaining statistically good bit sequences and usually deterministic functions called post-processing are applied to the output data.

Inherent randomness and indeterminacy provided by quantum physics can be exploited advantageously to generate random numbers. Quantum dots [5, 6], single photon avalanche photodiode (SPAD) [7], light emitting devices (LEDs) [8, 9], laser [10, 11], chaotic laser [12] , and atmospheric turbulence [13] have been employed as sources of entropy to produce random numbers. In this paper we present a quantum RNG (QRNG) based on silicon nanocrystals (Si-NCs) LEDs, able to produce statistically good bit sequences using a simple experimental setup for data extraction. Si-NCs LEDs have several advantages such as CMOS compatibility,

Integrated Photonics: Materials, Devices, and Applications III, edited by Jean-Marc Fédéli,
Proc. of SPIE Vol. 9520, 952004 · © 2015 SPIE · CCC code: 0277-786X/15/$18
doi: 10.1117/12.2179027

compactness, and equal cost as the standard LEDs which make them quite favorable for commercial applications.

Compared to some proposed alternatives with a simpler architecture [7] and higher bit-rate [10], our approach has some important advantages. As remarked by Certification Authorities (CA), a RNG has to provide a sufficiently accurate stochastic model describing the bit extraction mechanism within the generator. This is a necessary requirement in order to justify the probabilistic nature of the generator, and to be able to run live tests on the output to detect any possible mismatch between the designed and obtained behavior of the instrument. In [7] dark noise of the SPAD is used to generate events. Dark noise is difficult to be implemented in a probabilistic model and on the other hand the use of photons to stimulate events is a more robust scheme. Moreover the output of the RNG is not the sequence of observations of the entropy source, and the choice to output the least significant bit from each observation N is a processing of the real data.

The architecture proposed in [10] allows the generation of statistically good bits in a rather efficient way. However, before outputting bits from the source of entropy, a deterministic operation is performed to the APD signal; the bit-value "1" is associated with each event occurring in an even clock cycle, while the value "0" is associated with odd clock cycles. This is therefore equivalent to considering only the least significant bit of each event, as it is done in [7]. Even though the two above-mentioned approaches possess a simpler architecture and provide a higher bit-rate, our approach enjoys the advantages of the utilization of light instead of dark noise to stimulate events in the SPAD and the absence of a deterministic processing to the raw data. This implies the possibility to model efficiently the QRNG, while guaranteeing a truly random output relying only on quantum effects, without any deterministic features.

B. Description of the QRNG

B. I Theoretical

Assuming that the light emission is a Poisson process, the probability of not observing photons in a given time window t_w is given by the survival function of the exponential distribution. Suppose we fix t_w and that we want the probability of obserivng at least one photon to be equal to the probability of observing no photons, the survival function $e^{-\lambda t_w} = \frac{1}{2}$ implies $\lambda t_w = ln(2)$, where λ^{-1} is the average number of observed photons.

Repeating this experiment, we obtain a quantum RNG exploiting optics able to output 1 bit every t_w seconds. To do so we need a stable source of light, with no relevant drift in the photon flux, and a detector whose dark count rate is negligible [3]. The setup used for implementing this scheme is explained in detail in the next section.

B. II Experimental

The scheme for generating random bit sequences using silicon nanocrystals Si-NCs LEDs is shown in Fig. 1. The LED is driven by an adjustable current/voltage source (Agilent B1500A Semiconductor Device Parameter Analyzer). The light emitted from the LED is transmitted through an optical fiber assembly to a SPAD (PerkinElmer SPCM-AQRH-16) with an afterpulsing probability of 0.5%. This photodiode is connected to a multichannel scaler (Oretc Easy-MCS) in which the photon arrivals are recorded with the dwell time in each channel selectable from 100 ns to 1300 seconds and with no dead time between the channels. In our experiments we fixed a bin-width of $t_w = 1\mu s$.

The active layer of Si-NCs LED is a graded-size multilayer with specifications described in Anopchenko et al. work [14]. The electroluminescence (EL) as a function of current is presented in Fig. 2. Injection of carries into Si-NCs by direct tunneling or Fowler-Nordheim tunneling mechanisms results in the generation of electron-hole pairs inside the NC (by impact excitation or formation of exciton). The generated pairs recombine spontaneously emitting photons. Since the spontaneous emission of photons in a LED is a non-deterministic process, the Si-NCs LED can be used as a quantum source of randomness. As discussed in [15] to assure the injection of carriers into Si-NCs under the direct tunneling mechanism and to avoid the Fowler-Nordheim tunneling which causes degradation to the oxide layer and hence inefficiency of the LED, the applied forward current (negative bias) to the LED was lower than ~1.79 μA (corresponding to the voltage 3 V).

As can be seen in Fig. 2, at 1.79 μA the EL is about $8x10^5$ counts/sec which allows driving the LED with lower currents than 1.79 μA to obtain ~ $6.9x10^5$ counts/s for the bin-width of 1 μs. In order to get the equal probability of ones and zeros, the current was varied accordingly in the range of 1.5-1.6 μA with the resolution of 500 pA.

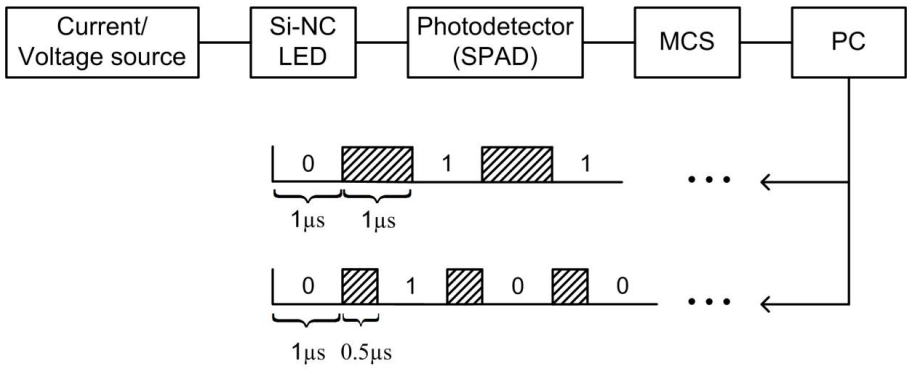

Fig. 1 Schematic diagram for generating random bit sequences with dead time simulation of 1 μs and 500 ns

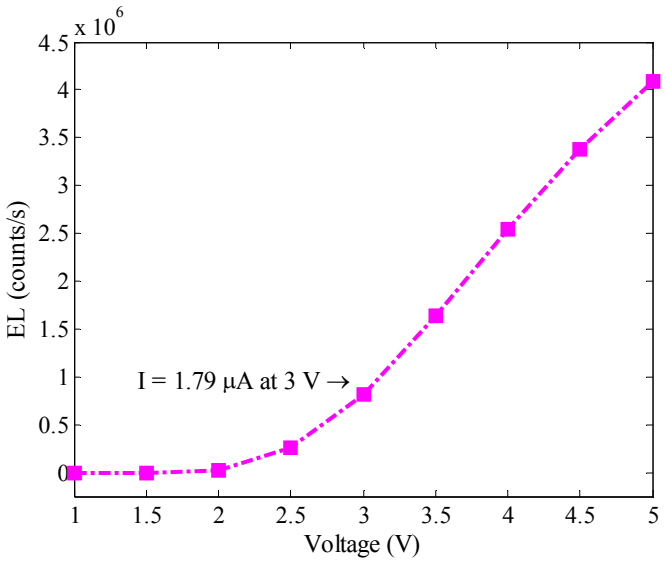

Fig. 2 EL as a function of voltage for Si-NC LED

C. Results

Several datasets were produced and analyzed. NIST test suite [16] uses a 99% confidence interval for the Frequency test, and recommends strings of at least 10^6 bits. One advantage of our setup is the negligible bias measured from the datasets. This allows the production of sequences to pass NIST Frequency test without any deterministic post-processing. Moreover, the only test in NIST test suite that fails with our setup is the Runs test.

Based on the structure of the runs test, which compares the probability of two consecutive bits being the same or not, and since we do not see any failure in any of the other tests, a likely explanation for this failure is the existence of correlation between consecutive bits in our datasets. By considering the sequences as the output of a Markov process of order one, we built the transition matrix T of the process; since the experimental setup was designed so as to make individual 0 and 1 equiprobable, the transition matrix was symmetric and its stationary distribution is consequently uniform. We could not measure a difference between the uniform distribution and the transition probability after only two steps T^2 which suggested that any correlation present was low enough that extending the dead time by a single observation window would be appropriate.

To simulate this process we removed a bit every two in each dataset, keeping for example all the bits in odd position. This is a simulation of experimentally enforcing a dead time of length equal to the bin-width t_w. Doing this we halve the bit-rate, outputting a single bit every $2\mu s$ instead of $1\mu s$. The statistical analysis done on these new sequences shows no correlation between the bits, and a perfect balance between zeros and ones. These datasets pass all statistical tests in NIST test suite (the analysis is done using datasets of 10^8 bits, namely 100 sequences of 10^6 bits). The results are presented in Table I.

Further experiments showed that with our setup, a dead time of 500 ns is enough to remove the correlation between consecutive bits, allowing us to produce random sequences with optimal properties without the application of any kind of post-processing.

In this way we obtain a QRNG able to produce perfect random data without the presence of any deterministic post-processing, with a bit-rate of 0.6 Mbps.

Table I Results of the NIST tests for 100 sequences of 10^6 bits for a simulated dead time of 1 μs

Statistical test	P-value	Proportion	Result
Frequency	0.554420	99/100*	Success
Block frequency	0.935716	100/100	Success
Cumulative sums	0.983453	99/100	Success
Runs	0.657933	99/100	Success
Longest run	0.964295	100/100	Success
Rank	0.911413	98/100	Success
FFT	0.514124	98/100	Success
Non-overlapping templates	0.514124	98/100	Success
Overlapping template	0.779188	100/100	Success
Universal	0.000700	100/100	Success
Approximate entropy	0.657933	100/100	Success
Random excursions	0.468595	64/64**	Success
Random excursions variant	0.028181	64/64	Success
Serial	0.262249	98/100	Success
Linear complexity	0.366918	100/100	Success

*The minimum pass rate for each statistical test with the exception of the random excursion (variant) test is approximately = 96 for a sample size = 100 binary sequences.

**The minimum pass rate for the random excursion (variant) test is approximately = 60 for a sample size = 64 binary sequences.

D. Conclusions

We realized a physical quantum random number generator exploiting Si-NCs LED as the source of randomness. Very negligible bias and simple setup are the chief strengths of our QRNG. With

the simulation of a dead time of 1μs and 500ns, the bit sequences pass all the statistical tests in NIST test suite. The highest bit-rate achieved via this QRNG is 0.6Mbps which is relatively low compared to existing physical RNGs. However, our approach benefits from of the utilization of light instead of dark noise to stimulate events in the SPAD and the absence of a deterministic processing to the raw data which is extremely remarkable in producing high quality random numbers and can compensate for the low bit-rate. As an additional point, it should be mentioned that higher bit-rates are expected by the parallelization of our system.

Acknowledgments

The research was funded by the Autonomous Province of Trento, Call "Grandi Progetti 2012", project "On Silicon chip quantum optics for quantum computing and secure communications - SiQuro".

References

[1] Ferrenberg, A.M., Landau, D. and Wong, Y. J., "Monte carlo simulations: Hidden errors from ''good''random number generators," Physical Review Letters 69, 3382 (1992).
[2] Resende, F. J. and Costa, B. V., "Using random number generators in Monte Carlo simulations," Physical Review E 58, 5183-5184 (1998).
[3] Gisin, N., Ribordy, G., Tittel, W. and Zbinden, H., "Quantum cryptography," Reviews of Modern Physics 74, 145-195 (2002).
[4] Lo, H.-K., Curty, M. and Tamaki, K., "Secure quantum key distribution," Nat Photon 8, 595-604 (2014).
[5] Stevenson, R., Thompson, R., Shields, A., Farrer, I., Kardynal, B., Ritchie, D. and Pepper, M., "Quantum dots as a photon source for passive quantum key encoding," Physical Review B 66, 081302 (2002).
[6] Naruse, M., Kim, S.-J., Aono, M., Hori, H. and Ohtsu, M., "Chaotic oscillation and random-number generation based on nanoscale optical-energy transfer," Sci. Rep. 4, 6039 (2014).
[7] Tisa, S. and Zappa, F., "One-chip quantum random number generator," SPIE OPTO: Integrated Optoelectronic Devices, International Society for Optics and Photonics, 72360J-72360J-72310 (2009).
[8] Wahl, M., Leifgen, M., Berlin, M., Röhlicke, T., Rahn, H.-J. and Benson, O., "An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements," Applied Physics Letters 98 (17), 171105 (2011).
[9] Sanguinetti, B., Martin, A., Zbinden, H. and Gisin, N., "Quantum Random Number Generation on a Mobile Phone," Physical Review X 4, 031056 (2014).

[10] Dynes, J.F., Yuan, Z.L., Sharpe, A.W. and Shields, A.J., "A high speed, postprocessing free, quantum random number generator," Applied Physics Letters 93, 031109 (2008).
[11] Qi, B., Chi, Y.-M., Lo, H.-K. and Qian, L., "High-speed quantum random number generation by measuring phase noise of a single-mode laser," Opt. Lett. 35, 312-314 (2010).
[12] Kanter, I., Aviad, Y., Reidler, I., Cohen, E. and Rosenbluh, M., "An optical ultrafast random bit generator," Nature Photonics 4, 58-61 (2010).
[13] Marangon, D.G., Vallone, G. and Villoresi, P., "Random bits, true and unbiased, from atmospheric turbulence," Sci. Rep. 4, 5490 (2014).
[14] Anopchenko, A., Marconi, A., Wang, M., Pucker, G., Bellutti, P. and Pavesi, L., "Graded-size Si quantum dot ensembles for efficient light-emitting diodes," Applied Physics Letters 99, 181108 (2011).
[15] Marconi, A., Anopchenko, A., Wang, M., Pucker, G., Bellutti, P. and Pavesi, L., "High power efficiency in Si-nc/SiO2 multilayer light emitting devices by bipolar direct tunneling," Applied Physics Letters 94, 221110 (2009).
[16] http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf.