Phys. Status Solidi A **213**, No. 12, 3186–3193 (2016) / **DOI** 10.1002/pssa.201600298

physica status solidi a
www.pss-a.com
applications and materials science

Generation of high quality random numbers via an all-silicon-based approach

Zahra Bisadi[*,1], Alessio Meneghetti[2], Alessandro Tomasi[2], Andrea Tengattini[1], Giorgio Fontana[1], Georg Pucker[3], Paolo Bettotti[1], Massimiliano Sala[2], and Lorenzo Pavesi[1]

[1] Nanoscience Laboratory, Department of Physics, University of Trento, Via Sommarive 14, 38123 Povo, Italy
[2] Department of Mathematics, University of Trento, Via Sommarive 14, 38123 Povo, Italy
[3] Center for Materials and Microsystems, FBK, Via Sommarive 18, 38123 Povo, Italy

Received 2 May 2016, revised 6 July 2016, accepted 15 July 2016
Published online 5 August 2016

Keywords NIST tests, quantum random number generation, silicon nanocrystals LED, Toeplitz-hashing extractor

[*] Corresponding author: e-mail zahra.bisadi@unitn.it, Phone: +39-0461-28-2941, Fax: +39-0461-28-3934

A quantum random number generator (QRNG) based on a silicon nanocrystals (Si-NCs) light emitting device (LED) coupled with a silicon single photon avalanche photodiode (Si-SPAD) is presented. A simple setup is used for the generation of random bits. The modeled approach assures a negligible bias on datasets of ∼100 Mbits length. The raw data pass all the statistical tests in the National Institute of Standards and Technology (NIST) suite without any post-processing operations. The bit-rate of 0.6 Mbps is achieved. The information-theoretically provable randomness extractor of Toeplitz-hashing function is applied to longer datasets (∼1 Gbits) to extract the randomness, to minimize the bias, and consequently pass all the NIST tests. Stabilizing the temperature, resetting the applied current to the LED, or a feedback system can also be used as parameter control solutions to generate good quality, long datasets of random numbers suitable for cryptographic applications.

1 Introduction

Encryption of data is of increasing importance and the use of random numbers is a common strategy to secure sensible data [1–5]. Providing cryptic messages completely protected from any eavesdropping is essential to guarantee secure data transmission. Random numbers are often obtained through pseudo random number generators (PRNG). They are deterministic algorithms that, starting from a deterministically generated seed (and hiding it using complex algorithms), generate sequences of pseudo-random bits. However, their unpredictability is not totally assured since when the seed is revealed, the entire sequence of bits can be produced [6]. The periodicity is also an undesirable property of PRNGs that can be disregarded for most practical purposes if the sequence recurs after a very long period. However, the predictability still remains a tremendous disadvantage.

The solution is to make use of physical nondeterministic phenomena. The chief assets of intrinsic indeterminacy and randomness in quantum physics can be utilized. Truly random numbers have been generated by exploiting the non-deterministic nature of quantum phenomena. Quantum dots [7, 8], single photon avalanche photodiode (SPAD) [9], light emitting devices (LEDs) [10–12], and laser [13–19] have been employed as sources of entropy to produce random numbers. Comparison of the number of photons in consecutive pulses of a coherent light source [17] and randomly varying exact number of photons in each laser pulse [16] have been proposed as photon counting approaches to generate random numbers. In some methods using attenuated laser [18, 19], the mean of the flux of photons is larger than one which makes the security of these methods arguable for applications in quantum cryptography [4]. The main limits to the implementation of physical RNGs are related to the realization of hardware able to output statistically good bit sequences. In [10], a 50/50 beam splitter is used to acquire sequences of data. However, since it is impossible to achieve perfect 50/50 coupling paths, they applied a certain mathematical procedure to unbias the raw data keeping the efficiency as high as possible. Thus, usually, the raw data have to be post-processed in order to remove correlations and bias effects [20–22].

In this paper, we introduce a quantum random number generator (QRNG) which is able to produce sequences of random bits with a very negligible bias that pass all the NIST tests without the need of a post-processing algorithm for small datasets (100 Mbits). It is based on silicon nanocrystals (Si-NCs) LED as the source of entropy coupled with silicon single photon avalanche photodiode (SPAD) as the detector. At low applied currents the Si-NCs LEDs act like an attenuated source of light with a Poisson distribution in photon counts statistics [24, 25]. Since the spontaneous emission of photons in Si-NCs LEDs is of nondeterministic quantum nature and considering the fact that these LEDs are CMOS compatible, employing them for the production of QRNGs is beneficial. The architecture where a Si LED and a Si SPAD are coupled can yield a compact and cheap QNRG fabricated by standard microelectronic processes. Furthermore, its performance can be greatly increased exploiting CMOS scalability.

For long datasets (1 Gbits) the problem of bias occurs which causes some of the main statistical tests in the NIST tests suite to fail. Different randomness extractors such as Von Neumann and XOR have been used to eliminate the bias and correlation in the raw datasets [21, 24]. However, the information-theoretically secure extractors need to be employed for privacy amplification in quantum key distribution (QKD) [23]. We implemented the Toeplitz-hashing function to remove the bias and correlation in long datasets in order to extract the randomness in the raw data. Some parameter control solutions are also suggested that would make possible the generation of long, high quality random bit streams.

2 Theoretical

2.1 Test for the Poisson distribution

Photons are emitted spontaneously in a Si-NCs LED. The spontaneous emission of photons in an LED is a non-deterministic, random process. In quantum electrodynamics, the atom-vacuum system, in the presence of the electromagnetic vacuum modes, is expressed by the superposition of the wavefunctions of the excited state atom with no photon and the ground state atom with a single emitted photon:

$$|\Psi(t)\rangle = \alpha(t)\mathrm{e}^{-i\omega_0 t}|e;0\rangle + \sum_{k,s}\beta_{ks}(t)\mathrm{e}^{-i\omega_k t}|g;1\rangle \tag{1}$$

where $|e;0\rangle$ and $\alpha(t)$ are the atomic excited state-electromagnetic vacuum wavefunction and its probability amplitude, $|g;1\rangle$ and $\beta_{ks}(t)$ are the ground state atom with a single photon wavefunction and its probability amplitude, ω_0 is the atomic transition frequency, and $\omega_k = c|k|$ is the frequency of the photon. k and s are the wavenumber and polarization of the emitted photon, respectively. A photon can be emitted with different wavenumbers and polarizations and thus a measurement on $|\Psi(t)\rangle$ results in a random projection to one of the eigenstates and its corresponding eigenvalue ω_k [26].

The randomness of photon arrival times makes it impossible to precisely define the number of emitted photons per unit time. Photons emitted through spontaneous emission follow a Poisson distribution with photons emitted independently from one another [27, 28].

There are several tests to examine whether a sample of observations comes from a Poisson distribution [29]. To test if the recorded data follows a Poisson distribution, we make use of the chi-squared (χ^2) statistic which compares observed data with the expected data we would obtain according to the null hypothesis that the data comes from a Poisson distribution. Let y_1, ..., y_n be independent, non-negative integer variables from a distribution P_1, the null and the alternative hypotheses then state that the distribution comes from a Poisson distribution P_2 or not, respectively:

$$H_1 : P_1 = P_2, \tag{2}$$

$$H_2 : P_1 \neq P_2. \tag{3}$$

The p-value which is the chi-square cumulative distribution function is calculated as [30]

$$P = \int_0^x \frac{t^{(d-2)/2}\mathrm{e}^{-t/2}}{2^{d/2}\Gamma(d/2)}\mathrm{d}t \tag{4}$$

where x is the calculated value of χ^2, d the degree of freedom and Γ the gamma function. Considering a significance level α, if the p-value is larger than this level (p-value $> \alpha$), the null hypothesis is accepted, otherwise the alternative hypothesis is accepted which indicates that the observed data does not come from a Poisson distribution.

2.2 Survival model

If the null hypothesis in subsection 2.1 is accepted, meaning that the photon counts show a Poisson distribution, the probability of not observing photons in a given time window t_w is given by the survival function with an exponential distribution. Let t denote the failure time of an individual from a homogeneous distribution, then the survival function is defined as the probability that t exceeds t_w [31]:

$$S(t_w) = \mathrm{Prob}(t > t_w) = \mathrm{e}^{-\lambda t_w}. \tag{5}$$

Suppose we fix t_w and that we want the probability of observing at least one photon to be equal to the probability of observing no photons, the survival function is then defined as:

$$\mathrm{e}^{\lambda, t_w} = \frac{1}{2} \rightarrow \lambda t_w = \ln(2), \tag{6}$$

where λ is the number of observed photons per unit time. In this way, by knowing the photon flux from an LED we can fix the integration time window of the multichannel scaler

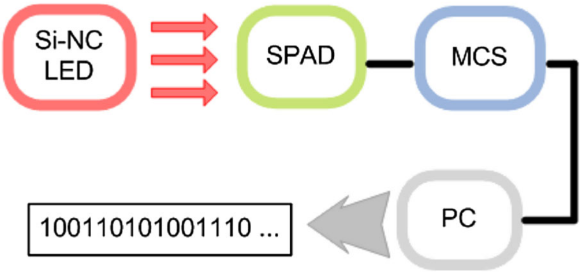

Figure 1 Scheme of the setup used to generate the bit sequences. Emitted photons from the silicon nanocrystals light emitting device (Si-NCs LED) are detected by a silicon single photon avalanche photodiode (SPAD). The electrical signals are then sent to a multichannel scaler (MCS) connected to a PC to generate sequences of random numbers.

connected to the detector to have an equal probability of detecting one photon and no photon.

2.3 Entropy In an ideal random sequence each bit is unpredictable and unbiased. The probability of observing each bit with a particular value is unaffected by the knowledge of the values of all the other bits. Entropy is intuitively defined as a measure of uncertainty. An ideal random sequence of n bits contains n bits of entropy.

The minimum entropy (min-entropy) is defined as the lower bound on the entropy of a random variable. It is often used as a worst-case measure of the unpredictability of observations y. The formula for the min-entropy for a given finite probability distribution, $p_1, ..., p_n$ is [32]

$$m = -\log(\max(p_1, ..., p_n)). \tag{7}$$

If y has min-entropy m, then the probability of observing any particular value is no greater than 2^{-m}.

3 Experimental Figure 1 shows the setup schematic for generating bit sequences using Si-NCs LED and Si SPAD. The current/voltage source that drives the LED is an Agilent B1500A Semiconductor Device Parameter Analyzer. The photons emitted from the LED are sent to the SPAD through an optical multimode fiber bundle which collects the light from the LED surface. No optics is used between the bundle and the LED. The SPAD is a PerkinElmer SPCM-AQRH-16, with the dead time of ~35 ns and after-pulsing probability of 0.5%. The pulses from the SPAD are recorded via a multichannel scaler Ortec Easy-MCS with a minimum channel (bin) width of 100 ns and with no dead time between the channels. The scan length is variable from 4 to 65,536 channels.

The Si-NC LED is based on a MOS structure where the gate oxide is formed by a 50 nm thick silicon rich silicon oxide which is activated by the presence of a graded-size Si-NC multilayer [33]. The electroluminescence (EL) as a function of applied current to the LED can be seen in Fig. 2. For these specific measurements, the EL spectrum was analyzed by a Spectra-Pro 2300i monochromator coupled with a

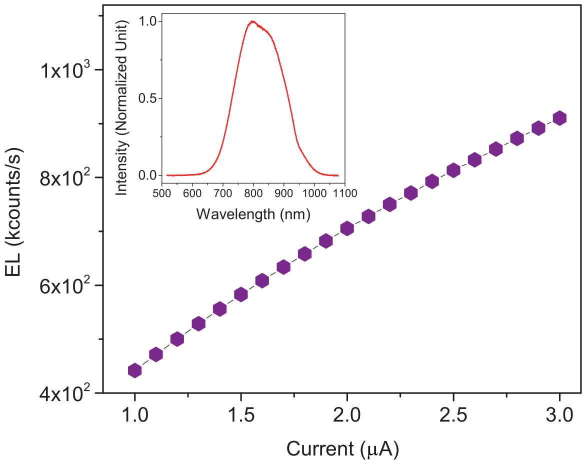

Figure 2 EL as a function of driving current to the Si-NCs LED. The inset represents the EL spectrum of the sample.

nitrogen-cooled charge coupled device (CCD) camera. The measurements were performed at room temperature in a dark room.

The LED characteristics are fully described in Ref. [33]. Briefly, 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 formation of exciton or impact excitation). The generated pairs recombine spontaneously emitting photons. As discussed in Ref. [34] 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 to the LED was kept lower than ~2.5 μA (corresponding to a voltage of 3 V). These LEDs show remarkable stability over week of continuous operation [35].

4 Results and discussion As stated before, since the spontaneous emission of photons in an LED is the origin of randomness, the Si-NCs LED can be used as a quantum source of randomness. First, we demonstrate that it can be described as a Poisson source. Having fixed the driving current, we measured the occurrence of counts in a time window t_w of 1 μs. The histogram plot of the counts with the Poisson fit is presented in Fig. 3. The statistics was done on 65535 counts recorded each two t_w (the reasons of this procedure was to remove correlations as we will detail later). Considering the conventional significance level of $\alpha = 0.05$, we computed a p-value of 0.0663. Since p-value $> \alpha$, we conclude that the Poisson distribution matches well with our obtained data.

The next step was then to make use of the survival function to fix the measurement parameters. The emitted photons from the Si-NCs LED were detected by the SPAD. The electrical signals out of the SPAD were then sent to the MCS with a maximum scan length of 65536 channel (bins) to count the input events (detected photons) in the channels of its digital memory. Fixing the bin width to 1 mus, we find

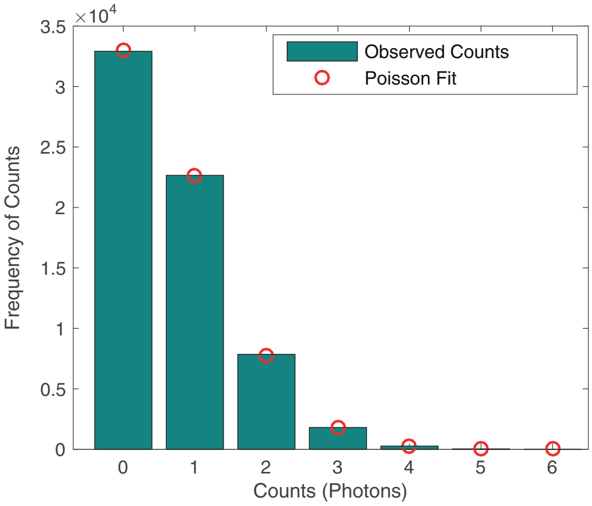

Figure 3 The histogram containing 65535 samples of data and the Poisson fit with the mean photon number of 0.69.

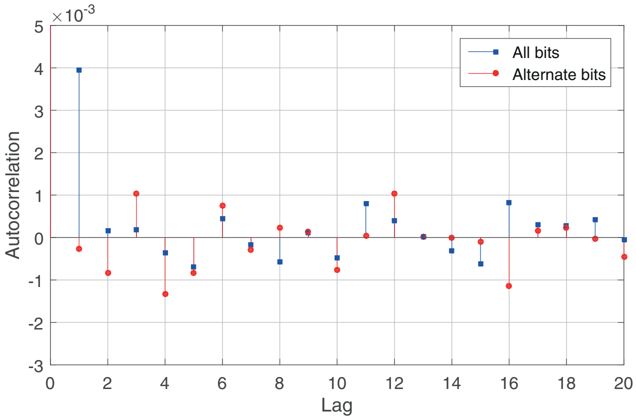

Figure 5 Autocorrelation versus time lag for the dataset of 262 sequences each of 10^6 bits (blue squares) showing high correlation at time lag 1 and the dataset of 131 sequences each of 10^6 bits (red circles) showing negligible correlation after eliminating each alternate bit in the dataset of 262 × 10^6 bits length.

$\lambda \sim 6.9 \times 10^5$ (counts/s) which implies that we have to apply a current of 1.8–2 μA to the Si-NCs LED (Fig. 2).

Fixing the applied current to the Si-NCs LED and acquiring data using the setup in Fig. 1, we measured the probability of ones for 262 sequences each of 10^6 bits (Fig. 4). The overall time duration of the sequences is then $262 \times 10^6 \times 1\ \mu s$ (i.e., number of sequences times number of bits times bin width), whereas the actual acquisition time was 28 min due to the time required for the data to be buffered in the MCS and transferred to the PC.

Then, the acquired bit strings were evaluated for randomness by a set of statistical tests. A very popular set is the NIST test suite [36]. The raw sequences passed all the statistical tests in the NIST tests suit except for the Runs test. This failure is usually attributed to the existence of correlation between consecutive bits since the Runs test implies that the probability of a change from 1 to a 0 to be equal to the probability of a change from 0 to 1 for a random sequence [36]. This correlation is caused by the detectors afterpulsing. As can be seen in Fig. 5 (blue squares), only the first time lag is correlated significantly since the time scale of the bin width is greater than the dead time of the avalanche photodiode [37].

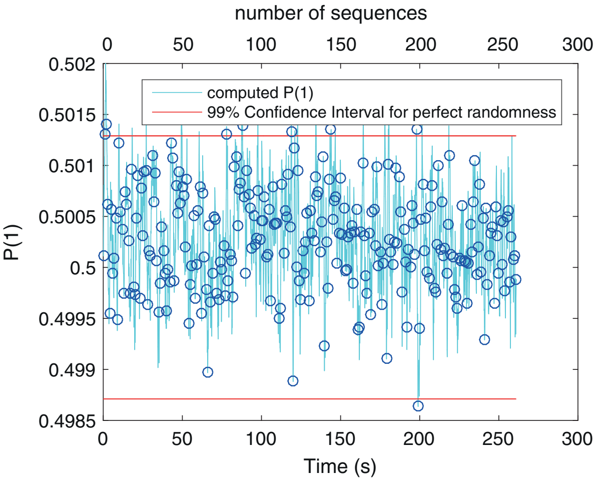

Figure 4 The evolution of the probability distribution of one with a 99% confidence interval in a dataset of 262 sequences each of 10^6 bits. Note that the time scale refers to the bit acquisition time and not the actual time of the measurement.

Considering the 262 sequences as the output of a Markov process of order one, we built the transition matrix T of the process. As mentioned before, the experimental setup was adjusted to make individual 0 and 1 equally likely to happen, so 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 suggests that any correlation present was low enough that reinforcing a dead time of a single observation window would be appropriate. Hence, one bit in every two in the dataset was removed that is like a simulation of experimentally enforcing a dead time of length equal to the bin width t_w. Doing so, we halve the bit-rate, outputting a single bit every 2 μs instead of 1 μs. The statistical analysis, done on these new sequences, shows no correlation between the bits and a perfect balance between zeros and ones. Figure 5 (red circles) represents the removal of the significant correlation after eliminating each alternate bit in the dataset. Therefore, the effect of the afterpulsing of the detector is removed.

The remaining 131 sequences of 10^6 bits (Fig. 6a) pass all the statistical tests in NIST test suite with a maximum measured bias of ~ 0.0012. The min-entropy is calculated to be ∼0.9965 bits per bit of data. To evaluate the success of the test, a significance level (α) of 0.01 is assigned for the test since common values of α in cryptography are about 0.01. If P-value$_T \geq 0.0001$, then the sequences can be considered to be uniformly distributed [36]. The proportion of passes

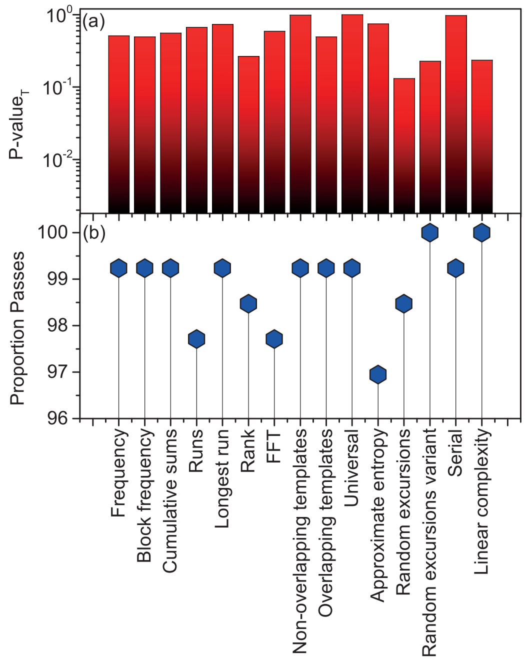

Figure 6 (a) Results of the NIST tests for 131 sequences of 10^6 bits for a simulated dead time of 1 μs. All tests are passed at the 0.01 significance level. (b) The proportion of passes for each test. The minimum pass rate for each statistical test is approximately 96 for a sample size of 100 binary sequences. The results of all tests have been normalized to 100.

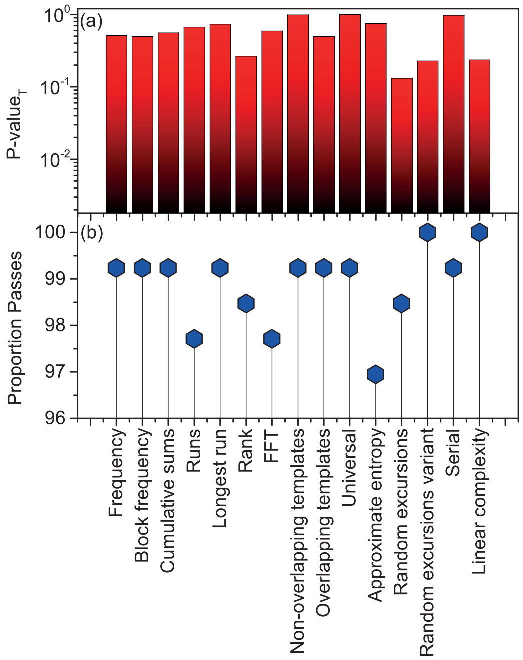

Figure 7 (a) Results of the NIST tests for 131 sequences of 10^6 bits for a simulated dead time of 500 ns. All tests are passed at the 0.01 significance level. (b) The proportion of passes for each test. The minimum pass rate for each statistical test is approximately 96 for a sample size of 100 binary sequences. The results of all tests have been normalized to 100.

for each test is presented in Fig. 6b. All the results have been normalized to 100.

It was shown after more experiments that to remove the correlation between consecutive bits in the dataset, an enforced dead time of 500 ns is sufficient. Doing so, high quality random sequences are generated without the application of any post-processing operations. The results of the NIST tests are illustrated in Fig. 7a and b.

5 Discussion on long dataset

The emission intensity of the Si-NCs LED is remarkably stable over continuous operation. Still small variations of the ambient conditions influence their behavior. Note that to acquire the 131 Mb long sequences that pass the NIST tests, we need to operate the system continuously for 28 min. This implies that the EL should be stable in that time interval. If we acquire 1 Gbits long sequences, the actual measurement time is about 214 min. Now EL dependence on ambient interference becomes evident (Fig. 9). In fact, considering a long dataset of 1 Gbits failure in the main statistical tests in NIST tests suite is observed which is due to the loss of equal probability of ones and zeros (bias) (Table 1). As shown in Fig. 8, a drift in the probability distribution of ones is observed. The failure time then precedes t_w and the survival function in Eq. (6) no longer applies to our system. The loss of the equal probability is due to a <0.4% variation in the EL of the Si-NCs LED. Figure 9a reports a day record of the emission intensity of the Si-NCs LED. Fluctuations of the EL intensity in the few per mille range are observed. At the same time, we have recorded also the voltage bias, the ambient temperature, and the ambient humidity (Fig. 9b, c, and d) to look for correlations. Close observation of the plots shows that the EL is most significantly correlated with the alterations of the ambient temperature. A slight decrease (increase) in ambient temperature results in a decrease (increase) in EL. It can be seen that after about 6 h of measurement, a small decrease of 0.5 °C in temperature causes a decrease of about 0.2% in the EL of the LED. As the bias factor increases exponentially with λ (Eqs. (4) and (5)), the randomness is extremely sensitive to the EL intensity and any small variation of the EL intensity will exponentially increase the bias factor. Therefore, the QNRG is possible only when the driving current is precisely set at each condition.

In the literature, to remove the bias on the data either a precise control on the QNRG parameters [10] or post-processing algorithms [20] or simple encoding methods [22] have been proposed. Although the boundary between post-processing algorithms and encoding methods is not clearly defined, the amount of resources needed can be adopted to differentiate. Here, we use the information-theoretically secure Toeplitz extractor [23] to extract the randomness in the raw dataset of 1 Gbits length. We implement the Toeplitz-hashing extractor to our QRNG as follows: as previously mentioned, the min-entropy of the raw data is ~0.99 bits per bit. With the input bit-string length of 1000 bits, the output bit-string length is $1000 \times 0.99 \geq 990$. Thus, the Toeplitz

Table 1 Results of the statistical NIST tests for the datasets of 1000 and 940 strings of 10^6 bits of raw and Toeplitz-extracted data, respectively. The P-value$_T$ has to be larger than 0.0001. The minimum pass rates for statistical tests is 0.98.

	raw data			Toeplitz-extracted data		
statistical test	P-value$_T$	proportion	result	P-value$_T$	proportion	result
frequency	0.000000	0.952	failed	0.114955	0.987	passed
block frequency	0.000000	0.968	failed	0.588505	0.992	passed
cumulative sums	0.000000	0.955	failed	0.229355	0.989	passed
runs	0.000000	0.431	failed	0.065561	0.988	passed
longest run	0.607993	0.992	passed	0.547061	0.984	passed
rank	0.916599	0.989	passed	0.164541	0.987	passed
FFT	0.130369	0.985	passed	0.601722	0.990	passed
non-overlapping template	0.009071	0.985	passed	0.855973	0.984	passed
overlapping template	0.000000	0.963	failed	0.676924	0.989	passed
universal	0.975012	0.990	passed	0.267060	0.990	passed
approximate entropy	0.000000	0.986	failed	0.100084	0.994	passed
random excursions	0.131334	0.980	passed	0.380164	0.984	passed
random excursions variant	0.034368	0.986	passed	0.182977	0.989	passed
serial	0.735908	0.984	passed	0.733513	0.989	passed
linear complexity	0.530120	0.993	passed	0.264222	0.990	passed

matrix of 1000 × 940 is conservatively used for randomness extraction. As can be seen in Fig. 10, the correlation is appreciably suppressed and all the NIST tests are passed for the Toeplitz-hashed dataset (Table 1).

Some parameter control solutions can also be taken into account for long datasets to overcome the drawback of the drift in the probability of ones (zeros) such as stabilizing the Si-NCs LED temperature, resetting the applied current to the Si-NCs LED (or equivalently resetting the bin width in the MCS), and designing a feedback for the system. Stabilizing the temperature, for instance, will cause the EL intensity to remain constant and therefore the equal probability of ones and zeros will be maintained. In the same manner, if the applied current to the LED or the bin width in MCS is reset

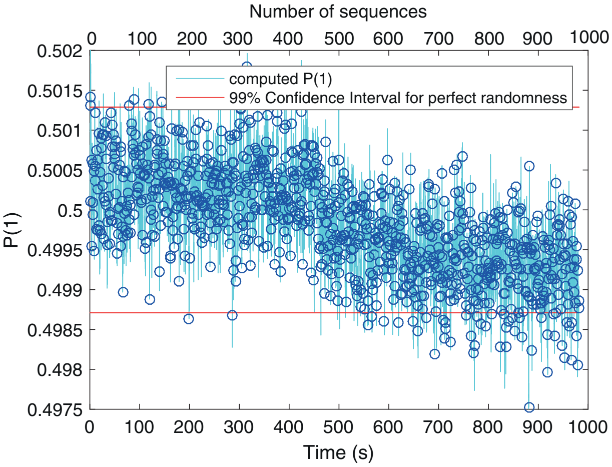

Figure 8 The evolution of the probability distribution of one with a 99% confidence interval in a dataset of 1000 sequences each of 10^6 bits. Note that the time scale refers to the bit acquisition time and not the actual time of the measurement.

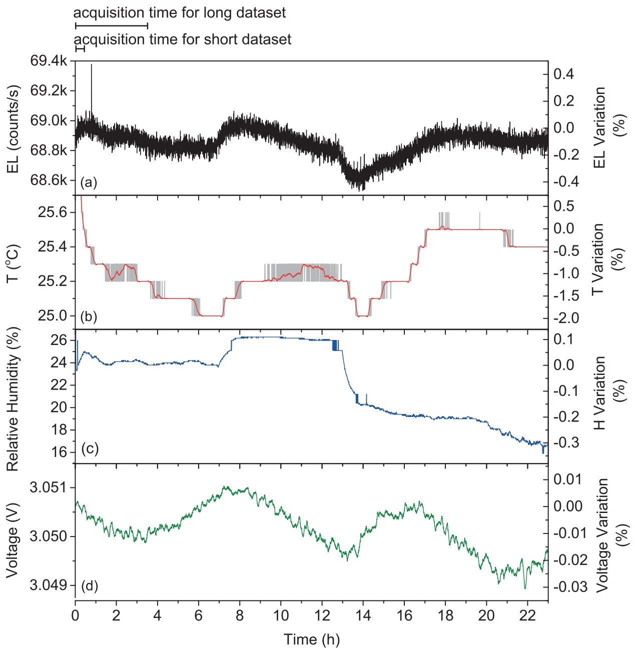

Figure 9 Plots showing (a) EL, (b) ambient temperature, (c) ambient humidity, and (d) Si-NCs LED voltage with their variations versus time. The acquisition time scales for small (28 min) and long (214 min) datasets can be seen on top of the plot.

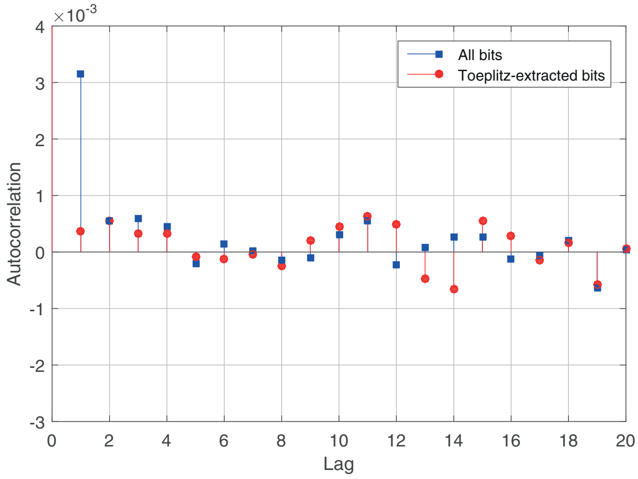

Figure 10 Autocorrelation versus time lag for 1 Gbits and 940 Mbits of raw data and Toeplitz-extracted data, respectively. The correlation at the first lag is minimized after the application of the Toeplitz extractor.

to keep the EL intensity invariant, the drift in the probability of ones (zeros) will be eliminated and eventually the system would produce long datasets of high quality random numbers. However, these methods are more resource hungry than the information-theoretically randomness extractors like the Toeplitz-hashing function.

6 Conclusion

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 forced dead time of 1 mus and 500 ns, 100 Mbits long sequences pass the statistical tests of the NIST suite. The highest bit-rate achieved is 0.6 Mbps. Despite the bit-rate, our approach benefits from several advantages: it uses light to stimulate events in the SPAD and avoids a deterministic post-processing of the raw data for small datasets. This fact is extremely remarkable in producing high quality random numbers and compensates for the low bit-rate. Furthermore, the approach proposed here uses simple silicon-based LEDs as the light source and its overall bit-rate can be easily increased by adopting a parallel architecture and exploiting the CMOS compatibility of all the components. However, 1 Gbits long datasets fail the main statistical tests in the NIST tests suite. This failure is attributed to a per mille drift in the EL of the Si-NCs LED that violates the equal probability of ones and zeros. The randomness is extracted by the application of the information-theoretically secure Toeplitz extractor. The bias and correlation among bits are removed and all the statistical tests in the NIST tests suite are consequently passed. A number of parameter control solutions such as stabilizing the temperature, resetting the applied current to the Si-NCs LED (or equivalently resetting the bin width in the MCS) and considering a feedback for the system can also be taken into account to overcome the problem of bias and to generate long, high quality random bit streams.

Acknowledgements This work was supported by Provincia Autonoma di Trento (PAT) through the call Grandi Progetti 2012: SIQURO.

References

[1] R. G. Heikes, D. C. Montgomery, and R. L. Rardini, Simulation **27**(3), 81–85 (1976).
[2] P. L'Ecuyer, Commun. ACM **33**(10), 85–97 (1990).
[3] L. Kocarevi, IEEE Circuits Syst. Mag. **1**(3), 6–21 (2001).
[4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbindeni, Rev. Mod. Phys. **74**(1), 145 (2002).
[5] G. Brumfiel, Nature **447**(7143), 372–373 (2007).
[6] A. M. Ferrenberg, D. Landau, and Y. J. Wong, Phys. Rev. Lett. **69**(23), 3382 (1992).
[7] R. Stevenson, R. Thompson, A. Shields, I. Farrer, B. Kardynal, D. Ritchie, and M. Pepper, Phys. Rev. B **66**(8), 081302 (2002).
[8] M. Naruse, S. J. Kim, M. Aono, H. Hori, and M. Ohtsu, Sci. Rep. **4** (2014).
[9] S. Tisa and F. Zappa, in: SPIE OPTO: Integrated Optoelectronic Devices, SPIE Proceedings, San Jose, CA, USA, 72360J–72360J (2009).
[10] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, J. Mod. Opt. **47**(4), 595–598 (2000).
[11] M. Wahl, M. Leifgen, M. Berlin, T. Röhlicke, H. J. Rahn, and O. Benson, Appl. Phys. Lett. **98**(17), 171105 (2011).
[12] B. Sanguinetti, A. Martin, H. Zbinden, and N. Gisin, Phys. Rev. X **4**(3), 031056 (2014).
[13] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **93**(3), 031109 (2008).
[14] B. Qi, Y. M. Chi, H. K. Lo, and L. Qian, Opt. Lett. **35**(3), 312–314 (2010).
[15] I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, Nature Photon. **4**(1), 58–61 (2010).
[16] Y. Jian, M. Ren, E. Wu, G. Wu, and H. Zeng, Rev. Sci. Instrum. **82**(7), 073109 (2011).
[17] M. Ren, E. Wu, Y. Liang, Y. Jian, G. Wu, and H. Zeng, Phys. Rev. A **83**(2), 023820 (2011).
[18] S. Tisa, F. Villa, A. Giudice, G. Simmerle, and F. Zappa, IEEE J. Sel. Top. Quantum Electron. **21**(3), 23–29 (2015).
[19] M. Applegate, O. Thomas, J. Dynes, Z. Yuan, D. Ritchie, and A. Shields, Appl. Phys. Lett. **107**(7), 071106 (2015).
[20] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H. K. Lo, Opt. Express **20**(11), 12366–12377 (2012).
[21] T. Durt, C. Belmonte, L. P. Lamoureux, K. Panajotov, F. Van den Berghe, and H. Thienpont, Phys. Rev. A **87**(2), 022339 (2013).
[22] F. X. Wang, C. Wang, W. Chen, S. Wang, F. S. Lv, D. Y. He, Z. Q. Yin, H. W. Li, G. C. Guo, and Z. F. Han, J. Lightwave Technol. **33**(15), 3319–3326 (2015).
[23] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, Phys. Rev. A **87**(6), 062327 (2013).
[24] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, Phys. Rev. Lett. **98**(1), 010503 (2007).

[25] J. Rarity, P. Owens, and P. Tapster, J. Mod. Opt. **41**(12), 2435–2444 (1994).

[26] H. Zhou, X. Yuan, and X. Ma, Phys. Rev. A **91**(6), 062316 (2015).

[27] R. P. Prasankumar and A. J. Taylor, Optical Techniques for Solid-State Materials Characterization (CRC Press, Boca Raton, 2011).

[28] Y.-Q. Nie, H.-F. Zhang, Z. Zhang, J. Wang, X. Ma, J. Zhang, and J.-W. Pan, Appl. Phys. Lett. **104**(5), 051110 (2014).

[29] L. D. Brown and L. H. Zhao, Sankhyā: Indian J. Statistics A 611–625 (2002).

[30] C. Walck, Handbook on Statistical Distributions for Experimentalists, 2007), Internal Report SUF-PFY/96-01, University of Stockholm, Stockholm, Sweden, http://www.stat.rice.edu/∼dobelman/textfiles/DistributionsHandbook.pdf.

[31] J. D. Kalbfleisch and R. L. Prentice, The Statistical Analysis of Failure Time Data (John Wiley & Sons, Hoboken, New Jersey, 2011).

[32] http://csrc.nist.gov/publications/nistpubs/80090a/sp80090a.pdf/

[33] A. Anopchenko, A. Marconi, M. Wang, G. Pucker, P. Bellutti, and L. Pavesi, Appl. Phys. Lett. **99**(18), 181108 (2011).

[34] A. Marconi, A. Anopchenko, M. Wang, G. Pucker, P. Bellutti, and L. Pavesi, Appl. Phys. Lett. **94**(22), 221110 (2009).

[35] A. Anopchenko, A. Marconi, F. Sgrignuoli, L. Cattoni, A. Tengattini, G. Pucker, Y. Jestin, and L. Pavesi, Phys. Status Solidi A **210**(8), 1525–1531 (2013).

[36] http://csrc.nist.gov/groups/st/toolkit/rng/documents/sp800 22rev1a.pdf/

[37] R. G. Brown, K. D. Ridley, and J. G. Rarity, Appl. Opt. **25**(22), 4122–4126 (1986).