Robust Quantum Random Number Generation With Silicon Nanocrystals Light Source

Zahra Bisadi, *Member, IEEE*, Giorgio Fontana, Enrico Moser, Georg Pucker, and Lorenzo Pavesi, *Fellow, IEEE*

***Abstract*—A robust quantum random number generation methodology has been developed and tested. The physical setup is based on a silicon nanocrystals light source coupled with a Si single photon avalanche diode driving a fully synchronous digital logic in a field-programmable gate array. After detailed analyses of the source and the detector, methods have been developed to make the nonidealities of the system and their consequent drawbacks decoupled from the quality of the generated random numbers. All the statistical tests in the national institute of standards and technology tests suite and the TestU01 Alphabit battery are consistently passed without a postprocessing operation on the raw data and without any feedback action on the photon source or any other parameter of the system. The maximum demonstrated bit-rate reaches 1.68 Mb/s, with an efficiency of 4 bits per detected photon. The modeling proves that the system is not influenced by variations of the internal and external parameters, such as the aging of the components and changing temperature.**

***Index Terms*—NIST tests, quantum random number generation, silicon nanocrystals LED, TestU01.**

I. Introduction

THE generation of random numbers is an important issue in secure communication. Modern cryptographic techniques require sequences of high quality random numbers. A large body of research has been done for the generation of random numbers through physical, non algorithmic methods. Classical physics has been exploited in thermal systems to generate random numbers [1], [2]. These approaches have a deterministic nature as they are solely based on classical physics. Quantum mechanics, on the other hand, with the uncertainty and unpredictability in quantum phenomena has considerably helped to develop efficient methods to produce unique, high quality random numbers suitable for cryptographic applications [3]–[8]. However, most approaches [4], [6] need to apply post-processing algorithms to the raw data in order to elevate the quality of random numbers.

Different operating principles have been employed in optical quantum random number generators (QRNGs) [5], [9]–[13]. Random numbers have been generated through encoding the number of photons and translating it into random bits [5], [14], detection of spontaneous Raman scattered photons by two detectors labeled as “0” and “1” [12], taking bits from sampling the interfering part of a laser waveform in an asymmetric Mach-Zehnder interferometer [11] and labeling the short path and long path of photon detections as “0” and “1”, respectively [9]. Some optical QRNGs have been developed using a beam splitter and multiple detectors [9], [15], [16]. Unequal losses, unmatched detection efficiencies and imperfections of these elements affect the random number distribution and will be fatal for the QRNG reliability.

A class of optical QRNGs based on the timing measurement of the photon arrivals has been proposed in literature [17]–[21]. Random bits have been extracted by comparison of the time difference between subsequent random events [17], comparison of the photon numbers in consecutive laser pulses distributed in time [19], random arrival times of photons on a single and an array of photodiodes [18], [21], and encoding the independent and uniformly distributed random phase time [20]. In [21], despite the high bit-rate, the mean of the photon flux is larger than one which makes the security of this method arguable for applications in quantum cryptography where the quality of random numbers is of higher importance than the speed. In [18], the exponential distribution of the arrival times of photons introduces bias in the raw data which is removed by post-processing operations. The bit extraction method in [17] makes the efficiency to be around 0.5 bits per detection since using the restartable clock method to eliminate both bias and correlation reduces the efficiency to less than 1 bit per arrival. In a recent method [20], with the maximum generation rate of 128 Mbps, the quality of random numbers is affected by a bias introduced at too high counting rates. In addition, the setup used in this approach is complex.

To improve the state of the art in terms of simplicity, robustness and random numbers quality, we developed a methodology based on the photon arrival time measurements with thorough consideration of the detector imperfections. This approach is simple and easy to model, all-silicon based, robust and able to generate high quality random numbers. We focus on a random number generation technique in which the source of entropy is quantum mechanical. It is a Si nanocrystals (Si-NCs) light emitting diode (LED) coupled with a silicon single photon avalanche diode (SPAD). A dedicated field-programmable gate array (FPGA) performs the random bit extraction. This approach avoids the use of post-processing algorithms used elsewhere [6], [18]. The proposed QRNG is robust against

Manuscript received July 28, 2016; revised November 16, 2016 and January 5, 2017; accepted January 13, 2017. Date of publication January 22, 2017; date of current version April 20, 2017. This work was supported by the Project “SiQuro.”

Z. Bisadi, G. Fontana, E. Moser, and L. Pavesi are with the Nanoscience Laboratory, Department of Physics, University of Trento, Trento 38123, Italy (e-mail: zahra.bisadi@unitn.it; giorgio.fontana@unitn.it; enrico.moser@unitn.it; lorenzo.pavesi@unitn.it).

G. Pucker is with the Advanced Photonics and Photovoltaics, Foundation of Bruno Kessler, Trento 38123, Italy (e-mail: pucker@fbk.eu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JLT.2017.2656866

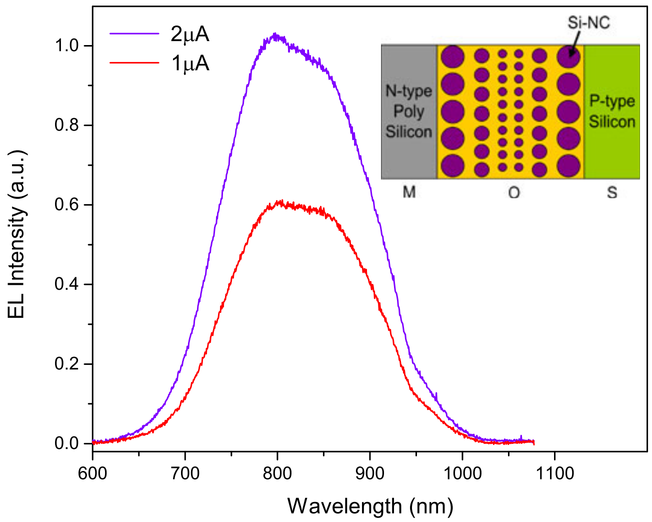

Fig. 1. The EL intensity of Si-NCs LED at two different applied current of 1 and 2 μA. The MOS structure of the Si-NCs LED with the graded-size multilayer active region is presented in the inset.

variations of the internal and external parameters such as the aging of the components and changing temperature. The components of the QRNG can be integrated on the silicon platform via complementary metal-oxide-semiconductor (CMOS) technology allowing the fabrication of a compact device.

II. Light Source and Photon Statistics

The Si-NCs LED has a metal-oxide-semiconductor (MOS) structure with a graded-size multilayer as the active layer (Fig. 1). They are formed by plasma-enhanced chemical vapor deposition (PECVD) inside the silicon-rich silicon oxide (SRO) layer. The SRO layers are confined between two 2 nm thick silicon dioxide (SiO_2) layers. Controlled thermal treatment causes the silicon precipitation in the SRO layer with the formation of Si-NCs [22]. The active area in the graded-size multilayer Si-NCs LED has stepwise thicknesses of 4-3-2-2-3-4 nm of SRO layers schematically shown in the inset of Fig. 1.

The multilayer has some advantages over a thick single layer including the formation of more uniformly-sized Si-NCs, higher density of Si-NCs, lower turn-on voltages and more efficient electroluminescence (EL) [22]. Larger Si-NCs near the two electrodes facilitate the carrier injection into the active region and smaller Si-NCs in the center of the structure make the emission more efficient since the radiative recombination rate increases as the size of NCs decreases. Full description of the characteristics of the Si-NCs LED can be found in [22].

Room temperature visible emission from excited excitons in the Si-NCs is observed when the MOS is forward bias (Fig. 1). The spectral region is particularly interesting since it matches the sensitivity of Si photodetectors. Emission power efficiency is small $\leq$0.5%. The injected current to the LED has to be $\leq$1.5-2 μA corresponding to a voltage of $\leq$ 3 V, so that the injection of carriers occurs through direct tunneling and the excitons are generated by bipolar injection of carriers. Above this threshold, unipolar injection occurs followed by impact ionization which causes a damage to the oxide layer due to the Fowler-Nordheim tunneling of hot carriers. The EL intensity of the Si-NCs LED is regulated by the injected current and suffers from aging or the influence of the ambient conditions [8], [22].

Statistical analysis on the number of photons emitted from the Si-NCs LED shows that it follows a nearly ideal Poisson distribution [8] with the mean photon number of 0.69. This property of the light source is used in the following sections.

III. Theoretical

A. *The Target Function*

The emission of photons from the LED follows a Poisson distribution. Therefore, the photon arrival on the SPAD can be described by Poisson statistics as well. The Poisson process has the property that if there is only one single arrival in a time interval [0, t], the distribution of the arrival times is uniform throughout the interval. This can be proved by writing the conditional probability and substituting the joint probability with independent probabilities of one photon detection in (0, τ] and no photon detection in (τ, t] [23]:

$$\begin{aligned} P(T \leq \tau \mid N(t) = 1) &= \frac{P(T \leq \tau, N(t) = 1)}{P(N(t) = 1)} \\ &= \frac{P(1 \text{ event in } (0,\tau], 0 \text{ event in } (\tau, t])}{P(N(t) = 1)} \\ &= \frac{P(1 \text{ event in } (0,\tau])P(0 \text{ event in } (\tau, t])}{P(N(t) = 1)} \\ &= \frac{\lambda\tau e^{-\lambda\tau} e^{-\lambda(t-\tau)}}{\lambda t e^{-\lambda t}} \\ &= \frac{\tau}{t}, \end{aligned} \tag{1}$$

where λ is the intensity of the process, i.e. the average number of arrivals per unit time. Thus we consider intervals with a fixed length having only one single arrival; intervals with no arrival or with more than one arrival are discarded. In this way we cope with the emission variations of the Si-NC LED at the expenses of a reduced random bit generation rate.

Since photon detection is done by a single photon avalanche photodiode (SPAD), the lack of photon number resolution causes the SPAD to make the measurements N $>$ 0 rather than N $=$ 1. However, the probability of photon arrivals, $P(T \leq \tau \mid N(t) > 0)$, tends to $P(T \leq \tau \mid N(t) = 1)$ for small λ and/or short time interval, making the probability of more than one arrival very negligible and keeping the previous consideration in Eq. (1) valid.

The interval and subinterval structure for an ideal detector is explained in Fig. 2(a). Every interval is composed of 16 subintervals of equal length, each associated with a symbol that generates the random number if a single photon is detected (i.e. a photon arrival occurs) in that specific time interval.

The real Si SPADs exhibit a number of non-idealities. The most important ones are afterpulsing, dead time, jitter, dark counts, light emission during avalanche and efficiency lower than 100%; all dependent on temperature, ageing, bias voltage, etc. Afterpulses are strongly correlated to true pulses and can severely deteriorate the Poisson statistics of the source.

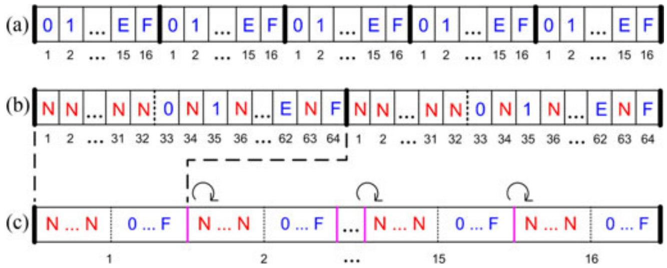
(a)
0 1 ... E F 0 1 ... E F 0 1 ... E F 0 1 ... E F 0 1 ... E F
1 2 ... 15 16 1 2 ... 15 16 1 2 ... 15 16 1 2 ... 15 16 1 2 ... 15 16
(b)
N N ... N N 0 N 1 N ... E N F N N ... N N 0 N 1 N ... E N F
1 2 ... 31 32 33 34 35 36 ... 62 63 64 1 2 ... 31 32 33 34 35 36 ... 62 63 64
(c)
N ... N 0 ... F N ... N 0 ... F ... N ... N 0 ... F N ... N 0 ... F
1 2 ... 15 16

Fig. 2. Schematic of (a) a conventional interval with 16 symbols of {0 1 2 ... 9 A B ... F}, (b) the "double length" interval with the first half of no number symbol (N) and the second half with N subintervals between symbols, and (c) the super interval containing 16 "double length" intervals as in (b) with a consecutive one-rotation of symbols.

Through autocorrelation analysis of the detector signal, the afterpulsing distribution can be measured. Dead time can also be measured with autocorrelation analysis of the detector signal. The detector jitter is a random variable that adds to the arrival times of the photons. Therefore, it changes the statistics of the measured arrival times.

Compared to the operational photon flux, dark counts are extremely rare events in our detector (~300 counts/s) and they do not alter the overall behavior of the apparatus. Detector efficiency is about 50% and simply adds to the losses of the whole optical chain. The low efficiency of the detector highlights the fact that a large proportion of the arrivals are inherently discarded by the losses. The surviving detections, however, keep their Poisson distribution.

In order to mitigate these detector non-idealities, we modified the simple scheme of Fig. 2(a). First, we consider the afterpulsing which occurs within a single interval; it causes multiple detections within the same interval. Since we discard all intervals with more than one detected photon, this kind of afterpulsing has no effect. Then, we take into account the afterpulsing which occurs across intervals (i.e. a photon is detected in an interval while the afterpulse is generated in the following time interval). It can be defeated by counting the number of photon arrivals in the previous interval. If there is one or more than one detection in the previous interval, the actual interval is discarded. Therefore, it may never happen that the afterpulse generated by a legitimate detection in an interval is counted as a legitimate detection in the following one. This mitigation strategy removes the effects of afterpulsing but reduces at the same time the efficiency of the generator.

The discard of an interval provided a photon detection in the previous interval, alleviates also across-interval dead time. In fact, if a legitimate photon is detected at the end of an interval and this arrival generates a random number, the detector dead time makes it impossible to detect a photon in the first subintervals of the following interval, introducing correlation in the random number generation. With the above-mentioned rule, this situation is impossible.

In-interval dead time can be masked if the dead time of the detector is shorter than the subinterval duration, so multiple photon detections would generate the same random number. Ideally, our method would discard that number due to more photon detections in an interval, but dead time makes it valid. This is equivalent to the effect of an optical attenuator, which does not alter the uniform distribution of arrival times. The case of in-interval dead time spanning across two subintervals is different; it changes the uniform distribution of arrival times. To overcome this problem, we introduce a no-number generating subinterval (nngs) between random number generating subintervals (rngs), as presented in Fig. 2(b). Doing so, in-interval dead time can mask photons that if detected would generate no number or would cause the number to be discarded, so again mimicking an optical attenuation.

One factor that might affect the results is the inability of the SPAD to resolve multiple photons arriving within the SPAD resolution window. Let us note that the result in Eq. (1) generalizes to any number of arrivals, i.e. if there are multiple arrivals in a time interval, each arrival time is a random variable with uniform distribution [23]. Therefore, if many photons hit the detector in the same resolution window, one of them should be selected at random before detection in order to be a valid photon according to our methodology. If multiple photons arrive at the same subinterval, one should be selected at random as mentioned before. However, multiple photons (not resolved by the detector) will generate the same random symbol as the single photon selected at random. In any case, a low flux of photons, obtained by an attenuator or a low efficiency source, makes this occurrence a low probability event. Thus, the inability to observe the multiple arrivals within the resolution window of the detector or inside the subinterval will not affect the generation method.

As mentioned before, the SPAD measures $N > 0$ and not $N = 1$. The two probabilities of $P(T \leq \tau \mid N(t) > 0)$ and $P(T \leq \tau \mid N(t) = 1)$ are merely different for large λ [23]. The observable departure from the uniform distribution (see Fig. 4) is possibly due to this phenomenon together with the non-uniform duration of the subintervals originated from the electronics as discussed below. We do propose in the following a mitigation technique which solves these issues.

Our methodology can be described in a compact form by defining "double length" periodic time intervals with an associated fully deterministic "target function". In the case of 16 rngs, the alphabet of the symbols is {N, 0, 1, ... F}, that reads N (no-number), and the hexadecimal numbers 0 to F. Each interval has 32 N subintervals in the first half and an alternation of N subintervals and the full set of numeric symbols in the second half, with a total of 64 subintervals [Fig. 2(b)]. Only if one single detection hits the target function associated with an interval, a random symbol is generated.

Through initial measurements, we observed a very small departure of $\sim 0.01\%$ in the probability of generated symbols from the ideal value of $P_{ideal}(symbol) = 1/16$ (see Section V) as the result of non-uniformity in the length of subintervals and/or the lack of photon number resolution in SPAD. The non-uniformity is most probably due to periodic fluctuations of rail voltages in the FPGA (the jitter) [24]. We have developed a mitigation technique in which each subinterval is assigned in advance and in a sequence to all symbols. The assignment is made before the possible arrival of a photon in an interval. The approach is called super interval structure as presented in Fig. 2(c). It is composed of 16 "double length" intervals, in which the random number generating symbols are ordered as {0, 1, ... F} in the first interval, {F, 0, ... E} in the second one and so on.

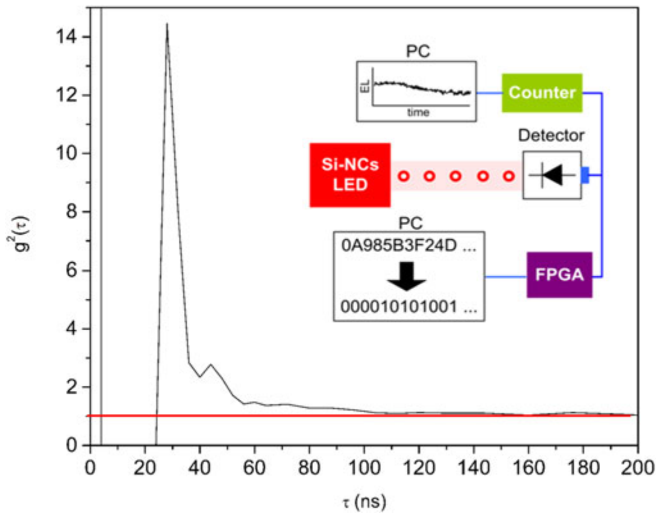

Fig. 3. Autocorrelation function ($g^2(\tau)$) of the detector signal (peak at zero is out of scale). Dead time and afterpulsing distribution of the detector can be seen here. The inset shows the schematic of the setup for random numbers generation. Photons emitted from a Si-NCs LED are detected by a single photon counting module (detector). The electroluminescence (EL) of the LED is monitored by a counter. The TTL output of the detector is connected to the high speed digital input of a field-programmable gate array (FPGA) which is connected to a PC for the acquisition of random sequences.

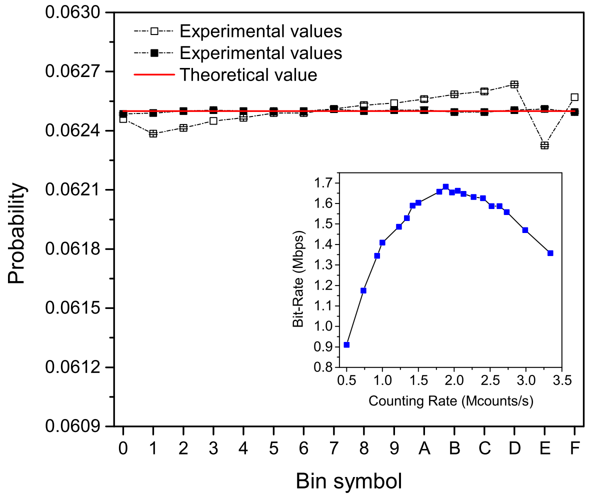

Fig. 4. Probability distribution of the 16 bin symbols built by analyzing 1G symbols raw data. The empty and filled squares refer to the experimental values obtained using target functions shown in Fig. 2(b) and (c), respectively, and the solid red line shows the theoretical value. The error bars are visible for some data points. The inset shows the experimental bit rate at different counting rates.

This approach fulfills the uniform probability distribution of the generated symbols (see Fig. 4 in Section V).

B. Robustness

Robustness plays a key role in a QRNG designed for cryptographic applications. The method employed to extract random numbers has to be robust against internal defects and external attacks. An external attack might change the dead time of the detector or the afterpulsing distribution, or it might find loopholes in the post-processing algorithms often used by most methods.

By masking the non-idealities of the detector described in the previous section, the internal robustness against the operational system defects is achieved. If the nominal characteristics of the light source and the Si SPAD are maintained within tolerances included in the design of the target function, the generation of high quality random numbers is guaranteed without any consistency check of the generation hardware. The external attacks could change the intensity of light by for instance a change in the temperature, but this effect will not change the quality of the random numbers; it might only change the efficiency of the generator (see Section V).

IV. Experimental

The experimental setup is presented in the inset of Fig. 3. Photons emitted from a Si-NCs LED are detected by a single photon counting module, PerkinElmer SPCM-AQRH-16, with timing resolution of 350 ps at FWHM, through a multimode fiber bundle. The LED is driven by an Agilent B1500A Semiconductor Device Parameter Analyzer. The electroluminescence (EL) of the LED is monitored by a Hewlett Packard 53131A Universal Counter 225 MHz by selecting the Totalize mode, so that true pulse counting is performed. The TTL output of the detector is directly connected to the high speed digital input of the FPGA.

The measurement of the arrival times is performed by a fully synchronous logic. The FPGA continuously samples the detector at the frequency of 100 MHz, which is crystal controlled. A valid arrival is produced by a high analog logic level heralded by one clock cycle (10 ns) of low analog logic level. A Digilent ATLYS FPGA board has been used with the programming language VHDL. The temperature is monitored and controlled by an LCI Light Control 350 Temperature Controller Module.

Autocorrelation, $g^2(\tau)$, measurement of the SPCM signal was performed via a multitau digital correlator with 4 ns resolution [25]. The afterpulsing distribution exhibits a main peak within 80 ns from the main autocorrelation peak at $\tau = 0$ (Fig. 3). Additional peaks are possibly related to reflections of the light generated by the SPAD itself when a photon is detected. This light pulse travels forth and back in the fiber and may induce a time shifted correlated detection. The plateau in $g^2(\tau)$ approaches the normalization value of 1 at about 160 ns.

We conservatively determined that after 320 ns afterpulsing and fiber reflections will not contribute to the statistics of the generated random numbers. Therefore, we adopt fixed contiguous "double length" time intervals of 640 ns, embedded in the super-interval structure. A single arrival in the second half of the interval [Fig. 2(b)] produces 4 bits when arrival occurs in one of the 16 possible active subintervals.

Starting with a Poisson process with intensity λ we need to assess the effect of considering only single arrivals in a time interval with minimum t_0 distance between the last rngs in interval M and the first rngs in interval M + 1. The distribution of the times (θ) between one arrival and the following one for a Poisson process is:

$$f_\theta(t) = \lambda e^{-\lambda t} \tag{2}$$

The integral over all times from 0 to ∞ gives 1. It means that the probability of having any possible elapsed time between one arrival and the following one is unity. If we exclude all arrivals that have inter-arrival time lower than t_0 and integrate between t_0 and infinity, we obtain $e^{-\lambda t_0}$. We can therefore define the average number of arrivals that have inter-arrival time greater than t_0 by multiplying the above probability by the average arrivals per unit time for the Poisson process:

$$\lambda_{t_0} = \lambda e^{-\lambda t_0} \tag{3}$$

It maximizes at $\lambda = 1/t_0$ with the value of λ/e. If λ is 1.56 Mcounts/s (corresponding to 1/640 ns), according to the theory (Eq. (3)) with t_0=320 ns the bit-rate would be 3.7 Mbps. However, the experimental bit-rate reaches 1.6 Mbps. This discrepancy depends on the losses due to N subintervals and on the detector dead time. The inset in Fig. 4 shows the experimental bit-rate at different counting rates. It reaches a maximum of about 1.68 Mbps at the counting rate of 1.88 Mcounts/s. At higher counting rates, the bit-rate decreases due to more discards of multiple arrivals in the time intervals.

V. Results and Discussion

A. Quality of Random Numbers

Using the setup shown in the inset of Fig. 3, long datasets were generated at different counting rates—equivalent to different applied currents to the Si-NCs LED—and different temperatures. The minimum counting rate is defined as the minimum count rate required having the buffer of the FPGA fully written.

It can be seen in Fig. 4 that the raw data, generated by the FPGA according to the procedure described, follow a uniform distribution which fits the expectation. Indeed, in the ideal case, the theoretical value for the probability distribution of 16 bin symbols is 1/16 (indicated by a solid red line in Fig. 4).

The generated raw data show high quality of randomness. Joint probability mass function (JPMF) [26], which is defined as the probability of having each symbol after the other one, is used to look for a potential weakness of this method. The analysis of JPMF shows a very low deviation in the order of $\sim 10^{-6}$ from the expected theoretical value of $(1/16) \times (1/16) = 0.00390625$ (Fig. 5). The mutual information (MI) of the generated random symbols is calculated by the formula below [27]:

$$I = \sum_{i=0}^{F} \sum_{j=1}^{F} P(i,j) \log \frac{P(i,j)}{P(i)P(j)} \tag{4}$$

where P(i, j) is the joint probability mass function of random variables i and j, and P(i) and P(j) are the marginal probability functions of i and j, respectively. The MI is calculated to be $\sim 10^{-7}$ bits considering 1G random symbols.

To test the robustness of our method, we arbitrarily changed the LED driving current or the LED temperature to change the emitted flux of photons. The min-entropy [28] of the raw data taken at different counting rates and temperatures is represented in Fig. 6(a) and (b), respectively. We observe that although it is slightly affected by the change in the counting rate of the photon flux and by the temperature variation, the values of the min-entropy are in the range of 3.99907-3.99972 bits per HEX digit (a nibble or 4-bits). This shows the high efficiency of our methodology with respect to entropy. The maximum bias is calculated to be in the order of $\sim 10^{-5}$.

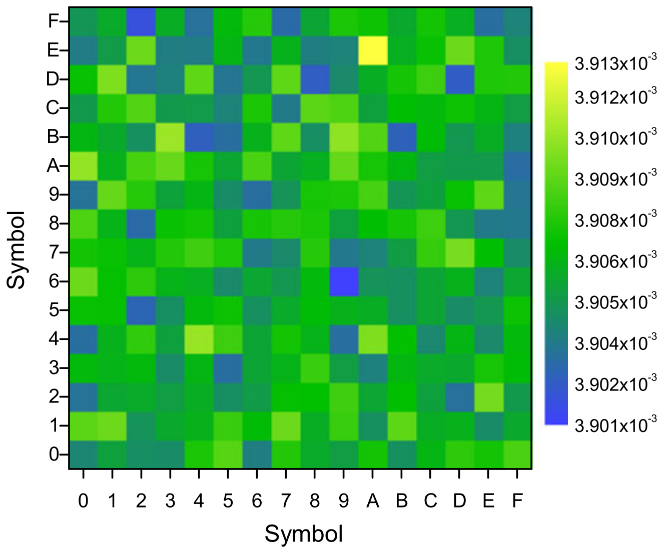

Fig. 5. Joint probability mass function for 1G generated symbols showing the probability of having each symbol followed by the other one.

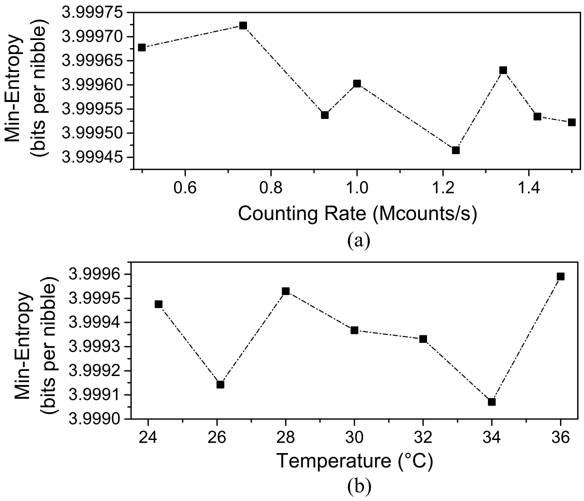

Fig. 6. Min-entropy of raw data sequences each containing 500 M symbols taken at a) different counting rates and b) different temperatures.

As mentioned before the legitimate detection of a photon in each subinterval produces 4 bits. Replacing each symbol with its corresponding 4-bit binary values, long sequences of zeros and ones are obtained.

The probability of having ones (zeros) is unaffected by the change of the photon flux or of the temperature (Fig. 7).

B. Statistical Tests

1) NIST Tests: We apply the 15 statistical tests in NIST tests suite to the generated raw data. Various datasets with 1 to 10 Gbits length at different applied currents to the LED —from the minimum counting rate to the maximum —and at different temperatures (24 °C - 36 °C) were obtained. They all passed the NIST tests without the application of a post processing algorithm irrespective of the EL variations of the LED during

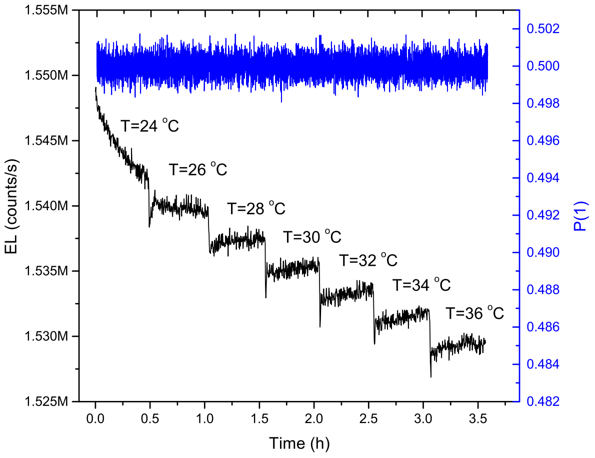

Fig. 7. The EL variation at different temperatures (black), the probability of ones (blue) can be seen on the right of the plot.

TABLE I
NIST TESTS RESULTS FOR 10G RANDOM BITS (10^{10} BITS)

Statistical test	P-value	Proportion	Result
Frequency	0.662506	0.9892	Passed
Block frequency	0.072289	0.9916	Passed
Cumulative sum	0.677444	0.9894	Passed
Runs	0.738917	0.9894	Passed
Longest run	0.067300	0.9910	Passed
Rank	0.322594	0.9910	Passed
FFT	0.291282	0.9870	Passed
Non overlapping template	0.581082	0.9909	Passed
Overlapping template	0.268110	0.9891	Passed
Universal	0.334077	0.9878	Passed
Approximate entropy	0.076564	0.9893	Passed
Random excursions	0.155778	0.9926	Passed
Random excursions variant	0.516352	0.9880	Passed
Serial	0.020945	0.9897	Passed
Linear complexity	0.025108	0.9902	Passed

The significance level is $\alpha = 0.01$. In order to pass, the p-value should be larger than 0.01 and the proportion should be more than 0.986.

data acquisition. The results for a dataset of 10 Gbits at the EL intensity of 1.5 Mcounts/s are reported in Table I.

2) Alphabit Battery: The Alphabit battery consists of 17 statistical tests designed primarily for hardware random bits generators. It is much faster than the NIST tests suite; it takes about 1 minute for 2^{30} bits of data [29].

We considered 200 datasets each of 1 Gbits length. The calculated p-values of the tests are presented in Fig. 8. In order to pass a test, the p-value has to be in the range of [0.001,0.9990]. If the deviation of p-value ($\Delta_{p-value}$=min{1− p-value, p-value}) is in the range of [10^{-6}, 10^{-2}], the test is considered inconclusive or weak and in the range of [10^{-15}, 10^{-6}] it fails [30].

The deviation of p-value for 4 tests (each one in a dataset) was $\sim 10^{-4}$ and hence they were considered weak. However, they are passed for all the other datasets. Statistically speaking, if we get the weak result for only one dataset out of 200, we can safely say that the test is passed consistently and the QRNG is considered ideal. All the tests were passed for all the other datasets.

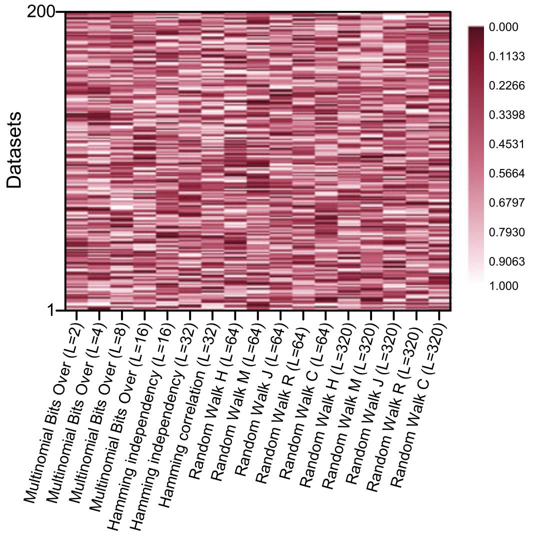

Fig. 8. The p-value of the 17 statistical tests in TestU01 Alphabit battery for 200 datasets each of 1 Gbits length.

VI. CONCLUSION

A robust methodology is developed to generate quantum random numbers. The source of entropy is a Si-NCs LED coupled with a Si SPAD connected to an FPGA to extract random numbers. So far in the literature, timing information of the photon arrivals has been utilized to generate random bits through different approaches. However, the lack of a robust methodology consisting of a complete study of the detector imperfections and a simple setup to generate random numbers has been evident. The methodology developed, tested and presented here masks all the defects of afterpulsing, dead time and jitter of the Si SPAD and is effectively insensitive to ageing of the LED and its emission drifts related to temperature. A simple, integrable setup is used to produce sequences of random numbers. Analyses of JPMF, MI and min-entropy show the high quality of generated random numbers and the high efficiency of the methodology. Despite the variations of the LED emission intensity, the system is efficient in producing long bit sequences maintaining the high quality of random numbers.

The raw data pass all the statistical tests in NIST tests suite and TestU01 Alphabit battery without a post processing algorithm. The maximum bit-rate we demonstrated is 1.68 Mbps with the efficiency of 4-bits per detected photon. The outlook for the future is integrating both the source and the detector in a single CMOS chip. Here, a compact configuration is possible when a single Si-NCs LED is coupled with a single Si SPAD (Si-NCs LED/Si SPAD).

The bit-rate can be increased by reducing the subintervals duration, optimizing the number of symbols per interval and decreasing the duration of the Ns between the random number generating subintervals, according to improved photodetector parameters. All these factors enhance the bit-rate at the expenses of a more complex and expensive system. Alternatively, parallelization can be employed to improve the generation rate; high bit-rate can be achieved by multiple Si-NCs LED/Si SPAD in a single chip. High density integration will benefit from the single detector structure and the use of very simple analog electronics not requiring silicon area for adjustment circuitries.

Acknowledgment

The authors would like to acknowledge fruitful discussions with Dr. A. Tomasi and A. Meneghetti from the Cryptolab of the University of Trento.

References

[1] A. Uchida *et al.*, “Fast physical random bit generation with chaotic semiconductor lasers,” *Nature Photon.*, vol. 2, no. 12, pp. 728–732, 2008.

[2] K. Hirano *et al.*, “Characteristics of fast physical random bit generation using chaotic semiconductor lasers,” *IEEE J. Quantum Electron.,* vol. 45, no. 11, pp. 1367–1379, Nov. 2009.

[3] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, “A high speed, postprocessing free, quantum random number generator,” *Appl. Phys. Lett.*, vol. 93, no. 3, 2008, Art. no. 031109.

[4] C. Gabriel *et al.*, “A generator for unique quantum random numbers based on vacuum states,” *Nature Photon.*, vol. 4, no. 10, pp. 711–715, 2010.

[5] B. Sanguinetti, A. Martin, H. Zbinden, and N. Gisin, “Quantum random number generation on a mobile phone,” *Phys. Rev. X*, vol. 4, no. 3, 2014, Art. no. 031056.

[6] Y.-Q. Nie *et al.*, “Practical and fast quantum random number generation based on photon arrival time relative to external reference,” *Appl. Phys. Lett.*, vol. 104, no. 5, 2014, Art. no. 051110.

[7] M. Stipčević and R. Ursin, “An on-demand optical quantum random number generator with in-future action and ultra-fast response,” *Sci. Rep.*, vol. 5, 2015, Art. no. 10214.

[8] Z. Bisadi, A. Meneghetti, G. Fontana, G. Pucker, P. Bettotti, and L. Pavesi, “Quantum random number generator based on silicon nanocrystals led,” in *Proc. SPIE*, 2015, Art. no. 952 004.

[9] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, “Optical quantum random number generator,” *J. Mod. Opt.*, vol. 47, no. 4, pp. 595–598, 2000.

[10] M. A. Wayne, E. R. Jeffrey, G. M. Akselrod, and P. G. Kwiat, “Photon arrival time quantum random number generation,” *J. Mod. Opt.*, vol. 56, no. 4, pp. 516–522, 2009.

[11] Z. Yuan, M. Lucamarini, J. Dynes, B. Fröhlich, A. Plews, and A. Shields, “Robust random number generation using steady-state emission of gain-switched laser diodes,” *Appl. Phys. Lett.*, vol. 104, no. 26, 2014, Art. no. 261112.

[12] M. Collins, A. Clark, C. Xiong, E. Mägi, M. Steel, and B. Eggleton, “Random number generation from spontaneous raman scattering,” *Appl. Phys. Lett.*, vol. 107, no. 14, 2015, Art. no. 141112.

[13] J.-m. Wang, T.-y. Xie, H.-f. Zhang, D.-x. Yang, C. Xie, and J. Wang, “A bias-free quantum random number generation using photon arrival time selectively,” *IEEE Photon. J.*, vol. 7, no. 2, pp. 1–8, Apr. 2015.

[14] M. Applegate, O. Thomas, J. Dynes, Z. Yuan, D. Ritchie, and A. Shields, “Efficient and robust quantum random number generation by photon number detection,” *Appl. Phys. Lett*, vol. 107, no. 7, 2015, Art. no. 071106.

[15] 2016. [Online]. Available: http://www.idquantique.com/wordpress/wp-content/uploads/white-paper-under standing-qkd.pdf

[16] M. Hai-Qiang *et al.*, “A random number generator based on quantum entangled photon pairs,” *Chin. Phys. Lett.*, vol. 21, no. 10, pp. 1961–1964, 2004.

[17] M. Stipčević and B. M. Rogina, “Quantum random number generator based on photonic emission in semiconductors,” *Rev. Sci. Instrum.*, vol. 78, no. 4, 2007, Art. no. 045104.

[18] M. Wahl, M. Leifgen, M. Berlin, T. Röhlicke, H.-J. Rahn, and O. Benson, “An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements,” *Appl. Phys. Lett.*, vol. 98, no. 17, 2011, Art. no. 171105.

[19] M. Ren, E. Wu, Y. Liang, Y. Jian, G. Wu, and H. Zeng, “Quantum random-number generator based on a photon-number-resolving detector,” *Phys. Rev. A*, vol. 83, no. 2, 2011, Art. no. 023820.

[20] Q. Yan, B. Zhao, Z. Hua, Q. Liao, and H. Yang, “High-speed quantum-random number generation by continuous measurement of arrival time of photons,” *Rev. Sci. Instrum.*, vol. 86, no. 7, 2015, Art. no. 073113.

[21] S. Tisa, F. Villa, A. Giudice, G. Simmerle, and F. Zappa, “High-speed quantum random number generation using CMOS photon counting detectors,” *IEEE J. Sel. Topics Quantum Electron.,* vol. 21, no. 3, pp. 23–29, May/Jun. 2015.

[22] A. Anopchenko, A. Marconi, M. Wang, G. Pucker, P. Bellutti, and L. Pavesi, “Graded-size Si quantum dot ensembles for efficient light-emitting diodes,” *Appl. Phys. Lett.*, vol. 99, no. 18, 2011, Art. no. 181108.

[23] S. M. Ross, *Applied Probability Models With Optimization Applications*. North Chelmsford, MA, USA: Courier Corporation, 2013.

[24] 2014. [Online]. Available: https://www.sitime.com/support2/documents/AN10007-Jitter-and-measurement. pdf

[25] S. Kalinin, R. Kühnemuth, H. Vardanyan, and C. A. Seidel, “Note: A 4 ns hardware photon correlator based on a general-purpose field-programmable gate array development board implemented in a compact setup for fluorescence correlation spectroscopy,” *Rev. Sci. Instrum.*, vol. 83, no. 9, 2012, Art. no. 096105.

[26] G. Grimmett and D. Stirzaker, *Probability and Random Processes*. London, U.K.: Oxford Univ. Press, 2001.

[27] R. M. Gray, *Entropy and Information Theory*. Berlin, Germany: Springer-Verlag, 2011.

[28] 2012. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf

[29] 2007. [Online]. Available: http://www.iro.umontreal.ca/~lecuyer/myftp/papers/testu01.pdf

[30] C. Abellán, W. Amaya, D. Mitrani, V. Pruneri, and M. W. Mitchell, “Generation of fresh and pure random numbers for loophole-free bell tests,” *Phys. Rev. Lett.*, vol. 115, no. 25, 2015, Art. no. 250403.

Zahra Bisadi received the B.S. degree in applied physics from Alzahra University, Tehran, Iran, in 2009 and the M.S. degree in solid state physics from Tarbiat Moallem University, Tehran, Iran, in 2011. She is currently working toward the Ph.D. degree at the Nanoscience Laboratory, University of Trento, Trento, Italy. Her main research interests include quantum optics, quantum random number generation, quantum information, and quantum communication.

Giorgio Fontana received the B.S. and M.S. degrees in electronic engineering from Padua University, Padua, Italy, in 1983. In 1984, he joined the University of Trento, Trento, Italy. He has authored or coauthored more than 50 refereed research publications. His current research focuses on the analysis and the development of applications of quantum optics, including quantum random numbers generators and instrumentation.

Enrico Moser received the certificates in electrotechnics and electronics in 1979 and electrotechnics and automation in 1998. From 1980 to 1989, he was a Technician in industrial fields and as a specialist in industrial electronics and automation.. In 1989, he joined the Department of Physics, University of Trento, as a Technologist (D3) in the UDR-TN. He worked in the field of design and setup of the optical and electronic instrumentation for the research activities of the Optical Spectroscopy and CNR groups until 2011. He has worked in the same field in the Nanoscience Laboratory, University of Trento, since 2011. He has more than 28 scientific articles in peer-reviewed journals and more than 40 oral and poster presentations in international conferences.

Georg Pucker is received the Ph.D. degree from the Technical University Graz, Graz, Austria, in 1996. He is currently a Senior Researcher of the CMM-FBK, Trento, Italy. He is the author of more than 90 scientific articles in peer-reviewed journals. His research interests range from photovoltaics, nanostructures, to integrated optical circuits.

Lorenzo Pavesi (F’17) is currently a Professor of experimental physics and the Head of the Department of Physics, University of Trento, Trento, Italy. He leads the Nanoscience Laboratory (25 people). He was the first President and the founder of the IEEE Italian chapter on nanotechnology. He has directed more than 30 Ph.D. students and more than 30 Master thesis students. His recent research interest focuses on integrated quantum photonics, neuromorphic photonics, and on-chip optical networks. He is an author or coauthor of more than 350 papers, author of several reviews, editor of more than 10 books, author of 2 books, and holds 7 patents. He is the Chief Specialty Editor of the section Optics and Photonics of Frontiers in Materials, on the editorial board of *Research Letters in Physics*, *Journal of Materials Science & Research,* and *Frontiers of Nanoscience and Nanotechnology*. In 2001, he received the title of Cavaliere by the Italian President for scientific merit. In 2010 and 2011, he was the elected distinguished speaker of the IEEE Photonics society. He is a Senior Member of SPIE. He holds an H-number of 52 according to the web of science or Scopus and of 64 according to Google Scholar.