A Robust Approach to the Generation of High Quality Random Numbers

Zahra Bisadi[a], Giorgio Fontana[a], Enrico Moser[a], Georg Pucker[b], and Lorenzo Pavesi[a]

[a]Nanoscience Laboratory, Department of Physics, University of Trento, Via Sommarive 14, 38123 Povo (Trento), Italy

[b]Center for Materials and Microsystems, Bruno Kessler Foundation, Via Sommarive 18, 38123 Povo (Trento), Italy

ABSTRACT

A random number generation approach comprising a silicon nanocrystals LED (Si-NCs LED), silicon single photon avalanche photodiode (Si SPAD) and a field-programmable gate array (FPGA) is introduced. The Si-NCs LED is the source of entropy with photon emission in the visible range detectable by silicon detectors allowing the fabrication of an all-silicon-based device. The proposed quantum random number generator (QRNG) is robust against variations of the internal and external parameters such as aging of the components, changing temperature, the ambient interferences and the silicon detector artifacts. The raw data show high quality of randomness and passed all the statistical tests in National Institute of Standards and Technology (NIST) tests suite without the application of a post-processing algorithm. The efficiency of random number generation is 4-bits per detected photon.

Keywords: Robust quantum random number generation, silicon nanocrystals LED, silicon single photon avalanche photodiode, field-programmable gate array, NIST tests suite

1. INTRODUCTION

High quality random numbers are required for modern cryptographic approaches. The generation of random numbers through physical, non algorithmic methods has been under research through years exploiting classical physics[1,2] and quantum physics.[3–8] Quantum phenomena with inherent uncertainty and unpredictability has been used to produce high quality random numbers. However, post-processing algorithms need to be applied to the raw data in most approaches[4,6] to improve the quality of random numbers.

Different optical quantum random number generators (QRNG) based on the timing measurement of the photon arrivals has been proposed in literature.[9–13] Random bits have been extracted by comparison of the time difference between subsequent random events,[9] comparison of the photon numbers in consecutive laser pulses distributed in time,[11] random arrival times of photons on a single and an array of photodiodes[10,13] and encoding the independent and uniformly distributed random phase time.[12] In Ref. 13, despite the high bit-rate, the mean of the photon flux is larger than one; hence the security of this method is arguable since in the application of quantum key distribution (QKD) in quantum cryptography, the quality of random numbers is more important than the speed. In Ref. 10, the bias in the raw data, caused by the exponential distribution of the arrival times of photons, is removed by post-processing operations. In Ref. 9, the efficiency is 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,[12] with the maximum generation rate of 128 Mbps, at too high counting rates the quality of random numbers is affected by a bias. In addition, the setup used in this approach is not very simple.

Further author information: (Send correspondence to Z. Bisadi)
Z. Bisadi: E-mail: zahra.bisadi@unitn.it, Telephone: +39 0461 28 2941
G. Fontana: E-mail: giorgio.fontana@unitn.it, Telephone: +39 0461 28 3906
E. Moser: E-mail: enrico.moser@unitn.it, Telephone: +39 0461 28 2001
G. Pucker: E-mail: pucker@fbk.eu, Telephone: +39 0461 31 4429
L. Pavesi: E-mail: lorenzo.pavesi@unitn.it, Telephone: +39 0461 28 1605

Quantum Information Science and Technology II, edited by Mark T. Gruneisen, Miloslav Dusek, John G. Rarity,
Proc. of SPIE Vol. 9996, 99960P · © 2016 SPIE · CCC code: 0277-786X/16/$18 · doi: 10.1117/12.2242000

Taking into account the simplicity, robustness and random numbers quality, we developed a methodology based on the photon arrival time measurements considering all the detector imperfections. This approach is simple and easy to model, all-silicon based, robust and able to generate high quality random numbers. It avoids the use of post-processing algorithms used elsewhere.[6,10] The proposed QRNG is robust against variations of the internal and external parameters such as aging of the components, temperature alterations, the ambient interferences and the silicon detector artifacts. The components of the QRNG can be integrated on silicon platform via complementary metal-oxide-semiconductor (CMOS) technology allowing the fabrication of a compact configuration. Our robust random number generation approach is based on a simple setup consisting of a silicon nanocrystals LED (Si-NCs LED), silicon single photon avalanche photodiode (Si SPAD) and a field-programmable gate array (FPGA).

2. METHODOLOGY

The Si-NCs LED generates photons through the quantum mechanical spontaneous emission process. Photons emitted from the Si-NCs LED follow a nearly ideal Poisson distribution.[8,14] 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. Theoretically, we can show this 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]:[15]

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

where λ is the average number of arrivals per unit time. Therefore, in our model, intervals with no arrival or with more than one arrival are discarded. Based on this, our main goals of robustness and full modeling of the QRNG will be achieved.

The interval and subinterval structure for an ideal detector is explained in Fig. 1(a). The intervals are placed consecutively one after the other. Every interval is composed of 16 subintervals, each associated with a hexadecimal symbol. If a single detected photon arrives at an interval, a random number is generated.

The Si SPAD has a number of non-idealities including 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. The detector jitter is a random variable that changes the statistics of the arrival times.

Compared to the operational photon flux, dark counts are extremely rare events in our detector ($\sim$ 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.

In order to mitigate these detector non-idealities, we modified the simple scheme of Fig. 1(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.

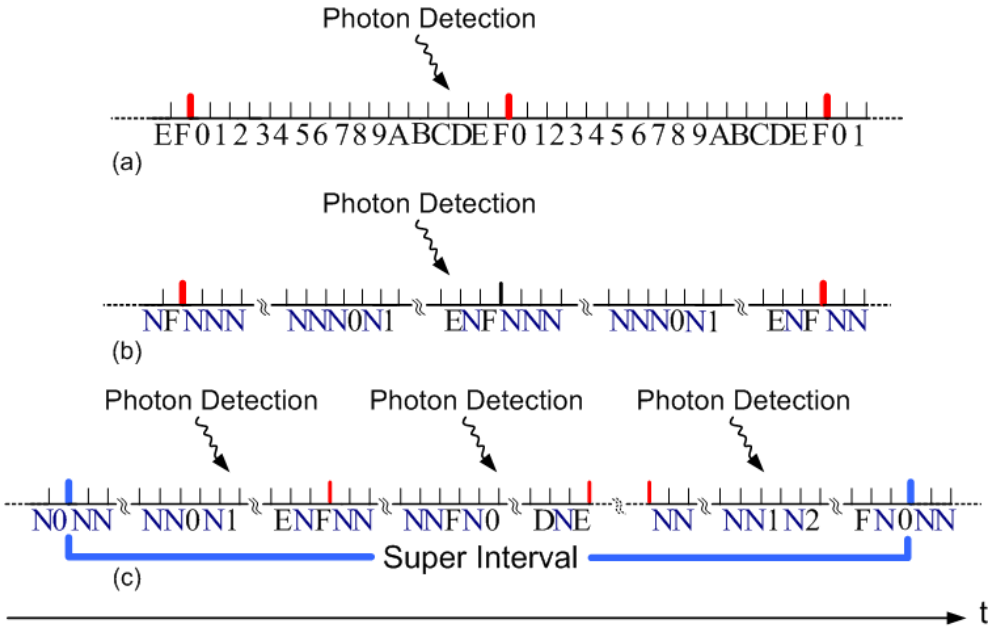

Figure 1. Schematic of (a) consecutive intervals with hexadecimal symbols, (b) the interval with the first half of no number symbol (N) and the second half with alternate N subintervals and hexadecimal symbols, and (c) the interval containing 16 intervals as in (b) with consecutive one-rotation of hexadecimal symbols.

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 (N) generating subinterval (nngs) between random number generating subintervals (rngs), as presented in Fig. 1(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.

Therefore, in order to overcome the non-idealities of the detector and the imperfections of the physical system:

i) A double length periodic time interval is introduced with no-number generating subintervals (nngs) between random number generating subintervals (rngs) (Fig. 1(b)). 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 (to mask the afterpulsing distribution of the Si SPAD) and an alternation of N subintervals and the full set of numeric symbols in the second half, with a total of 64 subintervals.

ii) A super-interval composed of 16 intervals is defined, in which the random number generating symbols are ordered as {0, 1, ... F} in the first interval, {F, 0, ... E} in the second and so on. The consecutive one-rotation of hexadecimal symbols does indeed uniformly redistribute the inherent jitter of the physical counter to all the hexadecimal symbols (Fig. 1(c)).

3. EXPERIMENTAL

The experimental setup is presented in Fig. 2. Photons emitted from a Si-NCs LED are detected by a single photon counting module (Si SPAD) through a multimode fiber bundle. The Si SPAD is connected to a field-programmable gate array (FPGA) to extract the random numbers. 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. 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.

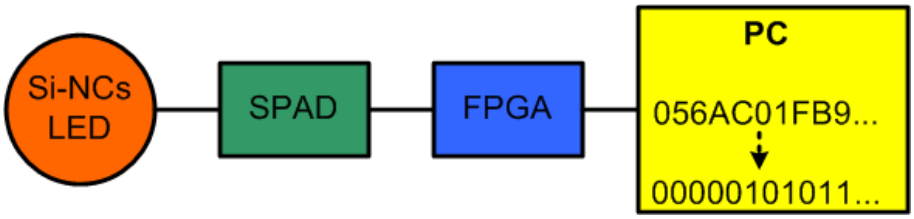

Figure 2. Schematic of the setup for random number generation. The photons emitted from the Si-NCs LED are detected by a Si single photon avalanche photodiode (SPAD) and then the electrical signals are sent to the FPGA where sequences of random symbols are produced. The random hexadecimal symbols are then converted into the binary 0 and 1 and hence sequences of 0s and 1s are generated.

4. QUALITY OF RANDOMNESS AND NIST TESTS

Sequences of data were obtained and analyzed for randomness. The raw data (acquired at different applied currents to the LED and different temperatures) show high quality of randomness. The analysis of the joint probability mass function (JPMF)[16]—that is the probability of having each symbol after the other one—shows a very low deviation in the order of $\sim 10^{-6}$ from the expected theoretical value of $(1/16) \times (1/16) = 0.00390625$. The mutual information (MI) of the generated random symbols is calculated by the formula:[17]

$$I = \sum_{i=0}^{F} \sum_{j=1}^{F} P(i,j) log \frac{P(i,j)}{P(i)P(j)} \tag{2}$$

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.

The hexademial numbers were then converted into 0 and 1 producing sequences of 0s and 1s (as seen in Fig. 2) to apply the NIST tests. all the sequences (taken at different temperatures and applied currents) passed all the statistical NIST tests[18] without the application of any post-processing algorithms. The result of the NIST tests are presented in Table 1 for 2G of random bits.

We changed the LED driving current or the LED temperature to change the emitted flux of photons (to test the robustness of our method). The min-entropy[18] of the raw data, taken at different counting rates and temperatures, was calculated. 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 hexadecimal 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 $\sim 10^{-5}$.

Table 1. NIST tests results for 2G random bits. The significance level is α=0.01. In order to pass, the p-value should be larger than 0.01 and the proportion should be more than 0.98.

Statistical test	**P-value**	**Proportion**	**Result**
Frequency	0.733899	0.9910	Passed
Block frequency	0.307077	0.9890	Passed
Cumulative sum	0.747898	0.9905	Passed
Runs	0.983697	0.9890	Passed
Longest run	0.344048	0.9925	Passed
Rank	0.820143	0.9890	Passed
FFT	0.115049	0.9890	Passed
Non overlapping template	0.703417	0.9835	Passed
Overlapping template	0.246750	0.9875	Passed
Universal	0.159464	0.9880	Passed
Approximate entropy	0.694171	0.9865	Passed
Random excursions	0.235410	0.9836	Passed
Random excursions variant	0.011014	0.9828	Passed
Serial	0.791565	0.9920	Passed
Linear complexity	0.296112	0.9925	Passed

5. CONCLUSIONS

A robust approach is introduced and tested 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. Timing information of the photon arrivals has been utilized to generate random bits through different approaches. A robust methodology consisting of a complete study of the detector imperfections and a simple setup to generate random numbers has not been reported in the literature. It masks all the drawbacks of afterpulsing, dead time and jitter of the Si SPAD. 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 EL variations of the LED, 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 without a post processing algorithm. We demonstrate that the maximum bit-rate 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.

ACKNOWLEDGMENTS

This work has been supported financially 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] Uchida, A., Amano, K., Inoue, M., Hirano, K., Naito, S., Someya, H., Oowada, I., Kurashige, T., Shiki, M., Yoshimori, S., et al., "Fast physical random bit generation with chaotic semiconductor lasers," *Nature Photonics* **2**(12), 728–732 (2008).

[2] Hirano, K., Amano, K., Uchida, A., Naito, S., Inoue, M., Yoshimori, S., Yoshimura, K., and Davis, P., "Characteristics of fast physical random bit generation using chaotic semiconductor lasers," *Quantum Electronics, IEEE Journal of* **45**(11), 1367–1379 (2009).

[3] 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**(3), 031109 (2008).
[4] Gabriel, C., Wittmann, C., Sych, D., Dong, R., Mauerer, W., Andersen, U. L., Marquardt, C., and Leuchs, G., "A generator for unique quantum random numbers based on vacuum states," *Nature Photonics* **4**(10), 711–715 (2010).
[5] Sanguinetti, B., Martin, A., Zbinden, H., and Gisin, N., "Quantum random number generation on a mobile phone," *Physical Review X* **4**(3), 031056 (2014).
[6] Nie, Y.-Q., Zhang, H.-F., Zhang, Z., Wang, J., Ma, X., Zhang, J., and Pan, J.-W., "Practical and fast quantum random number generation based on photon arrival time relative to external reference," *Applied Physics Letters* **104**(5), 051110 (2014).
[7] Stipčević, M. and Ursin, R., "An on-demand optical quantum random number generator with in-future action and ultra-fast response," *Scientific reports* **5** (2015).
[8] Bisadi, Z., Meneghetti, A., Fontana, G., Pucker, G., Bettotti, P., and Pavesi, L., "Quantum random number generator based on silicon nanocrystals led," in [*SPIE Microtechnologies*], 952004–952004, International Society for Optics and Photonics (2015).
[9] Stipčević, M. and Rogina, B. M., "Quantum random number generator based on photonic emission in semiconductors," *Review of scientific instruments* **78**(4), 045104 (2007).
[10] 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).
[11] Ren, M., Wu, E., Liang, Y., Jian, Y., Wu, G., and Zeng, H., "Quantum random-number generator based on a photon-number-resolving detector," *Physical Review A* **83**(2), 023820 (2011).
[12] Yan, Q., Zhao, B., Hua, Z., Liao, Q., and Yang, H., "High-speed quantum-random number generation by continuous measurement of arrival time of photons," *Review of Scientific Instruments* **86**(7), 073113 (2015).
[13] Tisa, S., Villa, F., Giudice, A., Simmerle, G., and Zappa, F., "High-speed quantum random number generation using cmos photon counting detectors," *Selected Topics in Quantum Electronics, IEEE Journal of* **21**(3), 23–29 (2015).
[14] Bisadi, Z., Meneghetti, A., Tomasi, A., Tengattini, A., Fontana, G., Pucker, G., Bettotti, P., Sala, M., and Pavesi, L., "Generation of high quality random numbers via an all-silicon-based approach," *physica status solidi (a)* (2016).
[15] Ross, S. M., [*Applied probability models with optimization applications*], Courier Corporation (2013).
[16] Grimmett, G. and Stirzaker, D., [*Probability and random processes*], Oxford university press (2001).
[17] Gray, R. M., [*Entropy and information theory*], Springer (2011).
[18] http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf.