High speed optical quantum random number generation

Martin Fürst[1,2,*], Henning Weier[1,2], Sebastian Nauerth[1], Davide G. Marangon[1], Christian Kurtsiefer[3] and Harald Weinfurter[1,4]

[1] *Fakultät für Physik, Ludwig-Maximilians-Universität München, D-80799 München, Germany*
[2] *qutools GmbH, D-80539 München, Germany*
[3] *National University of Singapore, Singapore 117543, Singapore*
[4] *Max-Planck-Institut für Quantenoptik, D-85748 Garching, Germany*
** martin.fuerst@qutools.com*

Abstract: We present a fully integrated, ready-for-use quantum random number generator (QRNG) whose stochastic model is based on the randomness of detecting single photons in attenuated light. We show that often annoying deadtime effects associated with photomultiplier tubes (PMT) can be utilized to avoid postprocessing for bias or correlations. The random numbers directly delivered to a PC, generated at a rate of up to 50 Mbit/s, clearly pass all tests relevant for (physical) random number generators.

OCIS codes: (270.5568) Quantum cryptography.

References and links

1. "Ais 20: Functionality classes and evaluation methodology for deterministic random number generators, v2.0, bsi," https://www.bsi.bund.de/cae/servlet/contentblob/478150/publicationFile/30276/ais20_pdf.pdf (1999).
2. "Fips 140-2, security requirements for cryptographic modules, nist," http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf (2001).
3. C. Petrie and J. Connelly, "A noise-based ic random number generator for applications in cryptography," IEEE Trans. Circuits Syst. I: Fundamental Theory and Applications **47**, 615–621 (2000).
4. W. Killmann and W. Schindler, "A design for a physical rng with robust entropy estimators," Lect Notes Comput Sc **5154**, 146–163 (2008).
5. B. Qi, Y. Che, H.-K. Lo, and L. Qian, "Experimental demonstration of a high speed quantum random number generation scheme based on measuring phase noise of a single mode laser," arXiv.org **0908.3351** (2009).
6. I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, "Ultrahigh-speed random number generation based on a chaotic semiconductor laser," Phys. Rev. Lett. **103**, 024102 (2009).
7. A. Alkassar, T. Nicolay, and M. Rohe, *Obtaining true random binary numbers from a weak radioactive source* (Springer-Verlag: Computational Science and its applitcations, 2005).
8. J. G. Rarity, P. C. M. Owens, and P. R. Tapster, "Quantum random-number generation and key sharing," J. Mod. Opt. **41**, 2435 (1994).
9. T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, "A fast and compact quantum random number generator," Rev. Sci. Instr. **71**, 1675–1680 (2000).
10. 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. **93**, 031109 (2008).
11. M. Stipcevic and B. M. Rogina, "Quantum random number generator based on photonic emission in semiconductors," Rev. Sci. Instrum. **78**, 045104 (2007).
12. S. Tisa and F. Zappa, "One-chip quantum random number generator" Proceedings SPIE **7236**, 72360J (2009)
13. O. Kwon, Y.-W. Cho, and Y.-H. Kim, "Quantum random number generator using photon-number path entanglement," Appl. Opt. **48**, 1774–1778 (2009).
14. P. Wang, G. Long, and Y. Li, "Scheme for a quantum random number generator," J. Appl. Phys. **100**, 056107 (2006).

#126957 - $15.00 USD Received 13 Apr 2010; revised 28 May 2010; accepted 1 Jun 2010; published 2 Jun 2010

15. A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, "Optical quantum random number generator," J. Mod. Optic. **47**, 595–598 (2000).
16. "Ais 31: Functionality classes and evaluation methodology for physical random number generators. v1.0," (2001).
17. W. Killmann and W. Schindler, "A proposal for: Functionality classes and evaluation methodology for true (physical) random number generators (v3.1)." https://www.bsi.bund.de/cae/servlet/contentblob/ 478134/publicationFile/30230/trngk31e_pdf.pdf (2001).
18. S. Prionio, "Random numbers certified by Bell's theorem," Nature **464**, 1021–1024 (2010).
19. R. J. Glauber, "The quantum theory of optical coherence," Phys. Rev. **130**, 2529–2539 (1963).
20. J. Soto, "Statistical testing of random number generators," Proc. 22nd National Information Systems Security Conference (1999).
21. R. G. Brown, "Dieharder test suite," http://www.phy.duke.edu/ rgb/General/dieharder.php (2009).
22. J. Kim and Y. Yamamoto, "Theory of noise in p-n junction light emitters," Phys. Rev. B **55**, 9949 (1997).
23. P. R. Tapster, J. G. Rarity, and J. S. Satchell, "Generation of sub-poissonian light by high-efficiency light-emitting diodes," EPL (Europhysics Letters) **4**, 293–299 (1987).
24. R. Loudon, *The quantum theory of light* (Oxford University Press, 2000), third edition ed.
25. R. Short and L. Mandel, "Observation of sub-poissonian photon statistics," Phys. Rev. Lett **51**, 384 (1983).
26. A. R. Dixon, J. F. Dynes, Z. L. Yuan, A. W. Sharpe, A. J. Bennet, and A. J. Shields, "Ultrashort dead time of photon-counting InGaAs avalanche photodiodes," Appl. Phys. Lett. **94**, 231113 (2009).
27. K. Omote, "Dead time effects in photon-counting distributions," Nucl Instrum Methods **293**, 582–588 (1990).
28. J. W. Mueller, "Some formulae for a dead-time-distorted poisson process," Nucl Instrum Methods **117**, 401–404 (1974).
29. D. E. Knuth, *The Art of Computer Programming II* (Addison-Wesley, 1998).
30. N. H. Kuiper, "Tests concerning random points on a circle," Proc. Kon. Ned. Aka Wet. **A 63**, 38–47 (1962).

1. Introduction

Random numbers are essential for a number of applications starting from lottery games, cryptographic applications such as generation of secure keys, or random numbers for secure personal identification, all the way to numerical simulations in physics. When calculated by algorithmic generators they are fully deterministic and necessarily exhibit a huge but finite period. Though they are quite frequently employed, care has to be taken for many applications [1, 2]. On the contrary, physical random number generators (RNG) avoid periodicity typical in algorithmic ones as their output results from generically stochastic processes. Measurements sample these processes pointwise in time, for example the Johnson noise in a resistor [3], the telegraph signal deduced from noisy Zehner diodes [4] or, more recently in an optical implementation, the phase noise fluctuation of a laser system [5, 6]. However, according to the laws of classical physics all these sources of noise are governed by perfectly deterministic dynamics. Only the complexity of the often chaotic evolution makes it impossible to predict the bit sequence with today's technology. Quantum physics provides inherent randomness and nondeterminacy. First designs of quantum random number generators used the spontaneous decay of radioactive nuclei as a non-deterministic quantum process [7]. Yet clearly photonic implementations are the tool of choice, as well developed optical components enable reliable and fast generation of random bits. First optical setups [8, 9] used the randomness of the detection of a single photon behind a beamsplitter. The registration of the photons in one or the other output of the beamsplitter was associated with the bit values '0' or '1', respectively. In these experiments different detection efficiencies of both detectors or the imperfect splitting ratio of the beam splitter lead to a preference of '0' or '1' and dead time effects caused correlations between consecutive bits. To remove the resulting bias and correlations, manipulation of efficiencies, post-processing algorithms and reduction of the sampling rate had to be used, which all significantly decreased the output rate. More recently a variaty of QRNGs was developed using different types of quantum randomness [8, 10, 11, 12, 13, 14, 15]. They all exhibit specific advantages, but often also one or the other disadvantage like low data rates, poor quality of raw random numbers either due to the bias or correlations along the bit sequence, and/or complex implementations. It should be also emphasized, that the standard test suites have to be used with care since they usually are

#126957 - $15.00 USD Received 13 Apr 2010; revised 28 May 2010; accepted 1 Jun 2010; published 2 Jun 2010

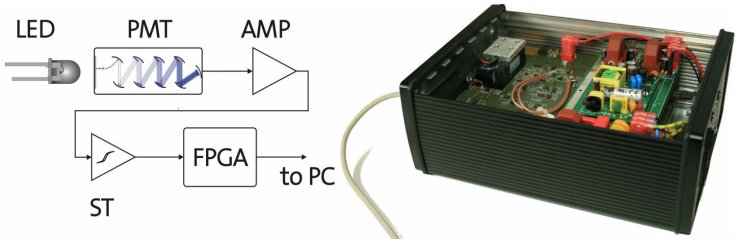

Fig. 1. Schematic of the setup (left) and picture of the fully integrated quantum random number generator (right). The main components are a light emitting diode (LED) mounted on the entrance window of a photomultiplier tube (PMT). The electrical pulses from the PMT are amplified (AMP) and fed into a threshold discriminator (ST). The signals are counted and processed by the FPGA, the resulting random bits are transferred to a PC via a USB connection. The total dimension of the housing is $22x16x8$ cm^3.

not optimized to detect typical problems of (quantum) physical RNGs such as bias, short time fluctuations, correlations and dropouts [16, 17]. Ultimately, the quantumness of random number generators might be certified in a device independent manner by Bell's theorem, currently though only at very low rates [18].

Here we present an optical QRNG, whose randomness is based on the very principles of quantum physics. The compact setup consists of a light source with stabilized intensity attenuated to the single photon level and one single photon detector. The detection events are counted during a sampling time interval τ_s and are interpreted as '0' for an even number of counts, whereas an odd reading corresponds to '1'. According to fundamental laws of quantum optics the probability distribution of the number of photons in a sampling interval should follow a Poissonian distribution with mean μ for a constant intensity light source [19], fully analogous to radioactive sources for low μ. This fact would cause a considerable bias between the number of '0's and '1's in the random bit sequence. However, as we demonstrate below, dead time effects of the photomultiplier together with the read-out electronics allow to eliminate the bias even for very fast generation of random bits. In addition to passing standard test suites [20, 21] for the evaluation of a physical random number generator [16] a stochastic model is required [17, 4]. Based on the concept outlined above here we describe the essential ingredients of such a model as well as the relevant tests of our implementation, clearly showing its suitability as a high rate optical QRNG.

2. Principle and setup

In the optical setup (Fig. 1) the constant light source is provided by a light emitting diode (LED) driven in cw-mode with digital feedback stabilization to about 1 ‰. The photon distribution emitted by the LED could be influenced by the Coulomb blockade effect inside the p-n-junction of the LED [22, 23], but, given the very weak coupling to the detector on the order of 10^{-8}, this effect can be neglected and the resulting distribution of photons falling on the detector is essentially Poissonian [24, 25]. To achieve high rates of random numbers we use a photomultiplier tube (PMT) instead of often used avalanche photodiodes (APD), as the long dead time of the latter on the order of $50-1000$ ns, characteristic for Geiger-mode operation, would significantly reduce the rate of random bits. Alternatively one might consider self differencing readout of APDs [26]. A PMT on its own has no such dead time in the single photon detection regime. There, the generation of a photoelectron and its subsequent amplification in the electron multiplier stages is in principle independent from any preceding processes. Yet,

#126957 - $15.00 USD Received 13 Apr 2010; revised 28 May 2010; accepted 1 Jun 2010; published 2 Jun 2010

the time of flight distributions of the photoelectrons and of the secondary electrons inside the PMT-module lead to an electrical pulse width on the order of a few nanoseconds (see inset in Fig. 2). A threshold discriminator used to convert the analog output pulse of the PMT into a digital signal can distinguish two pulses only, if they are separated by about the pulse width. This leads to an effective dead time τ_d, which even is *extendable* in the high intensity regime where more and more pulses start to overlap [27]. In order to finally produce the random bits the output of the discriminator circuit is fed into an FPGA logic (Spartan 3, clock speed 50 MHz). There, the counter, the periodic sampling procedure and on-the-fly functionality tests [17, 4] are implemented, and the random bits are transmitted to a PC via a USB connection.

Let us analyze the consequences of the dead time effects on the performance of the QRNG. For fully independent detection events with a mean rate of μ within the sampling interval τ_s, the probability to register n clicks is given by a Poisson distribution (Fig. 2)

$$P(n,\mu) = \frac{\mu^n}{n!} e^{-\mu} \ . \tag{1}$$

This distribution becomes modified when using a PMT. Due to the (extendable) dead time the initially Poissonian distribution of absorbed photons is significantly distorted by a factor depending on the mean number of *registered* events μ_r and the ratio between sampling time τ_s and dead time of the PMT τ_d. It is given by [27, 28]

$$P(n,\mu_r) = \underbrace{\frac{\mu_r^n}{n!} e^{-\mu_r}}_{\text{Poisson}} \cdot \underbrace{\sum_{k=0}^{K-n} \frac{(-\mu_r)^k}{k!} e^{\mu_r} \cdot \left((1-(k+n-1)\frac{\tau_d}{\tau_s})\right)^{n+k}}_{\text{extendable dead time modification}}, \tag{2}$$

with K

$$K = \left\lceil \frac{\tau_s}{\tau_d} \right\rceil$$

being the maximum detectable number of photons within the time interval τ_s. Figure 2 displays the change in the distribution relative to the Poisson distribution if the number of counts is close to K. While the mean decreases from μ to $\mu_r = \mu \cdot \exp(-\mu\,\tau_d/\tau_s)$ the probability for obtaining higher number of events is drastically reduced.

As the output of the QRNG results from an even/odd number of detection events within the sampling time interval, any change in the distribution of counts will influence the statistics of the random bits, and can cause artefacts, most remarkably bias or correlations. The probability for the random bit '0' (p_0) and '1' (p_1) can be calculated from Eq. (2). A bias b results from an unequal number of '0's and '1's and is given by

$$b = \frac{1}{2} - p_1 = \frac{1}{2} - \sum_{n=1,3,\ldots}^{\infty} P(n,\mu). \tag{3}$$

Clearly, the asymmetry of the Poisson distribution results in a bias, which only slowly reduces with increasing mean photon number. Thus, for this type of QRNG, postprocessing or sampling over longer times would become necessary. Both measures reduce the output rate of random bits. The dead time modified distribution Eq. (2), however, exhibits significantly different symmetry properties. Figure 3 compares the bias Eq. (3) resulting from the modified distribution Eq. (2) with the one due to a Poisson process. We observe that the bias of the modified distribution rapidly drops to and oscillates around 0, and is smaller by orders of magnitude over a wide range of mean number of detections. In the implementation of the generator this enables one to choose high rates with negligible bias and without serious sensitivity on fluctuations of the illumination intensity.

#126957 - $15.00 USD Received 13 Apr 2010; revised 28 May 2010; accepted 1 Jun 2010; published 2 Jun 2010

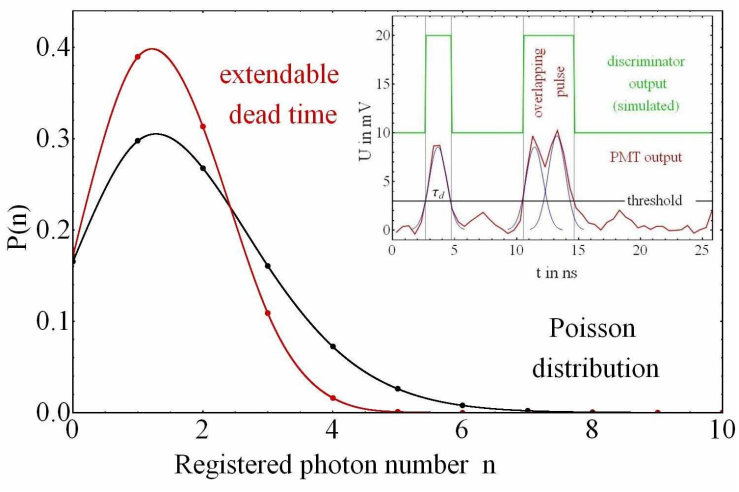

Fig. 2. Normalized distributions of detected photon numbers (calculated). The black line shows the distribution for a Poisson process with mean $\mu = 4.8$, i.e. without considering dead time effects. The red graph shows the expected distribution for an (extendable) dead time of the PMT of $\tau_d = 2.7$ ns and a sampling interval of $\tau_s = 20$ ns. This results in a strongly modified distribution, now with a mean $\mu_r = 2.51$ (see text). Lines are guide to the eyes. The inset exhibits the origin of the extendable dead time, where overlapping PMT pulses are not resolved anymore by the threshold electronics.

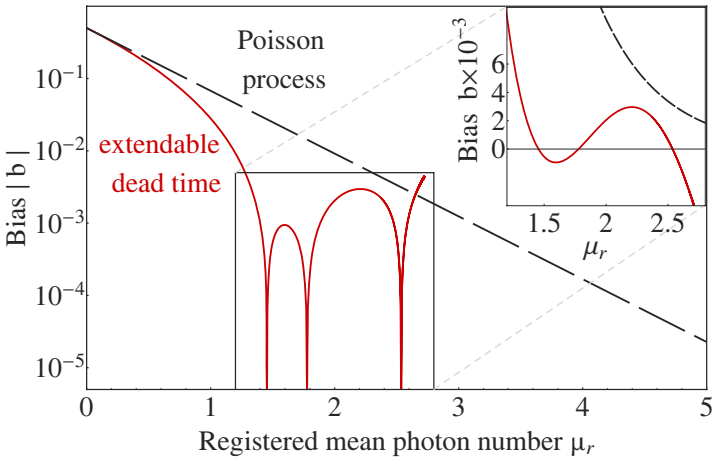

Fig. 3. Comparison between the dependency of the modulus of the bias of a random bit string on the detected mean photon number for an ideal Poisson process and for a process with extendable dead time. For this plot the dead time was chosen to be $\tau_d = 2.7$ ns and the sampling frequency to be $\tau_s = 20$ ns. The inset is a linear plot of the region of interest.

#126957 - $15.00 USD Received 13 Apr 2010; revised 28 May 2010; accepted 1 Jun 2010; published 2 Jun 2010

3. Evaluation and tests

Physical RNGs require new evaluation methods particularly in order to monitor the continuity of the stochastic process [16, 17]. For that purpose online tests for a coarse functionality inspection [16] are implemented in the FPGA logic and regularly performed on strings of 1 Mbit at intervals of one minute. These tests include the monobit-test and a chi-square test analyzing bias and statistics of 4-bit patterns, respectively, as well as a total-failure test. So far no excess fluctuations or degradation in the quality of the random bits was observed by these test routines.

To evaluate the performance of the actual implementation we have first analyzed the dependence of the bias on the mean number of detections (Fig. 4a) using 8 Gbit bit strings in order to obtain a statistical uncertainty as small as $3.2 \cdot 10^{-5}$ (dashed line). For sampling time intervals τ_s of $20, 40$ and 80 ns these measurements are compared to the theoretical predictions. From these measurements also the minimal dead time τ_d was extracted to be $\tau_d = 2.7$ ns by fitting the bias Eq. (3) to the data points.

The experimental result shows good agreement with the theoretical predictions and the effect of the extendable dead time reducing the bias was clearly verified. At higher detection rates (μ_r/τ_s) some deviation was caused mostly by the fact that this rate is beyond the specifications of the PMT ($< 50 \cdot 10^6$ events/s). Nevertheless, operating the QRNG around the first zero crossing of b enables one to obtain a performance consistent with what is to be expected for finite samples.

In addition, an important parameter of random numbers is the interdependence between consecutive bits. Contrary to algorithmic ones, physical random number generators are particularly susceptible to short time fluctuations, which easily can cause correlations. For that reason a dedicated analysis of the serial correlation coefficient SSC_l depending on the bit distance l of a bit sequence $b_1 \ldots b_N$ [29] has to be performed in addition to applying conventional random number test suites.

The correlation analysis of a 40 Gbit random bit string taken at a sampling interval of 20 ns and a mean photon number of $\mu_r = 1.41$ is shown in figure 4b. For all bit distances l we observe small values below $2 \cdot 10^{-5}$. This fully complies with the statistical predictions as, albeit the magnitude of this sample, there are finite size effects which cause fluctuations of the SCC_l, even for perfectly uncorrelated data of the same magnitude.

For further evaluation, bit strings of 1 Gbit obtained at a rate of 50 Mbit/s were analysed with two batteries of statistical tests: The "Statistical Test Suite" (STS) [20] from NIST and the "DieHarder" (DIE) test suite [21] for the same operating parameters as before.

The STS battery consists in total of 15 independent tests. Each individual test, resulting in p-values evaluated on 1 Mbit substrings, is performed 1000 times. A p-value gives the probability that a perfect random number generator would produce the actual one or a worse result. A final χ^2 test is applied on the p-value distribution of each individual tests which results in a total p-value (see Fig. 5). In order to appraise these results a significance level α is chosen. A typical value for this parameter is $\alpha = 1\%$, (labeled by the black line in Fig. 5). P-Values above this significance level indicate that the test is passed by the bit sequence generated by the QRNG.

The "DieHarder" battery of tests is a collection of 19 individual tests. Unlike in the STS tests, here a final Kuiper Kolmogorov-Smirnov Test [30] is performed giving p-values for each test separately. Again, the same level of significance is applied also to these results. The p-values from all tests are clearly above the significance level and therefore all the tests of the two test suites analysing the randomness of the output of our QRNG are passed.

#126957 - $15.00 USD Received 13 Apr 2010; revised 28 May 2010; accepted 1 Jun 2010; published 2 Jun 2010

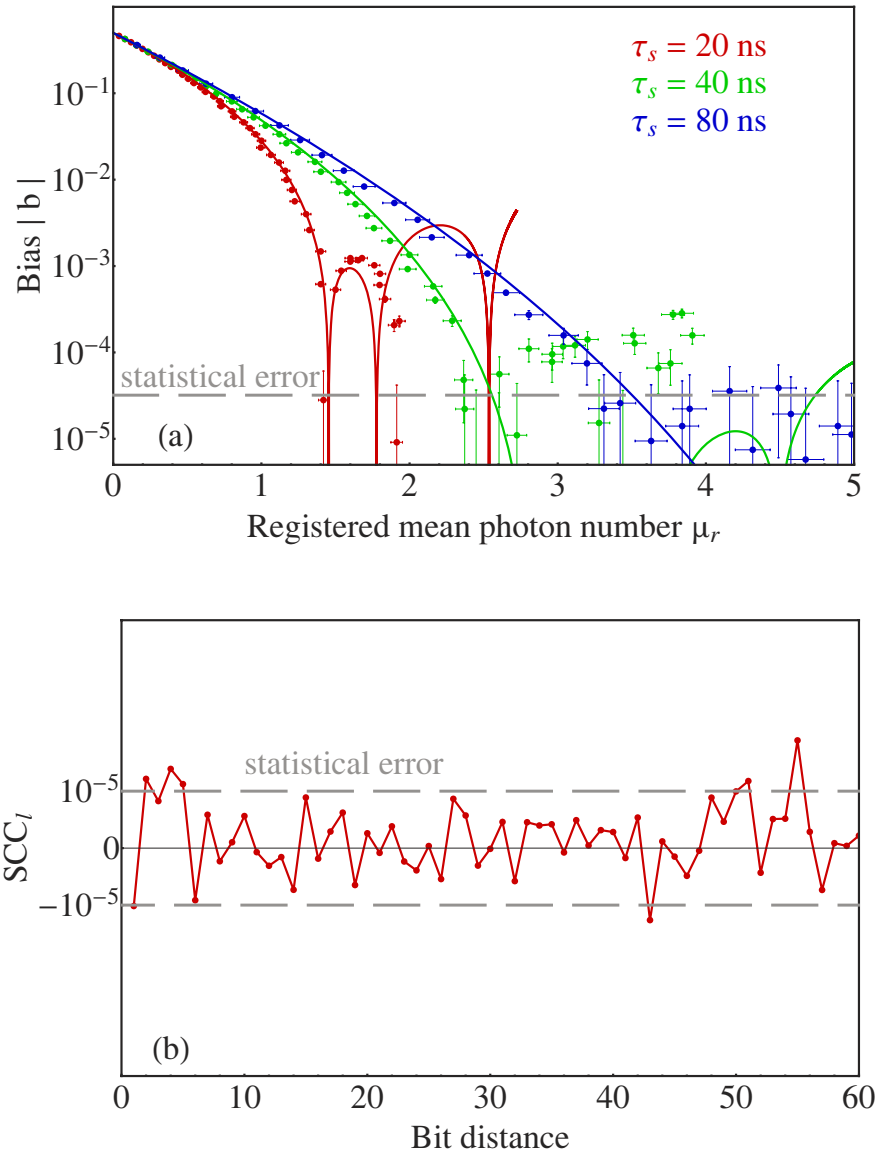

Fig. 4. Measurement of the bias depending on the mean number of detected photons (a). Each data point is obtained from an 8 Gbit bit string for three different sampling times. Serial correlation coefficient SCC_l of a single 40 Gbit string, collected with a sampling time of $\tau_s = 20$ ns and a mean photon number of $\mu_r = 1.41$, as a function of the bit distance (b). The statistical error levels shown in the plots are the 3-σ variance of the bias b or the SCC_l to be expected for an ideal random bit sequence with finite sample length.

#126957 - $15.00 USD Received 13 Apr 2010; revised 28 May 2010; accepted 1 Jun 2010; published 2 Jun 2010

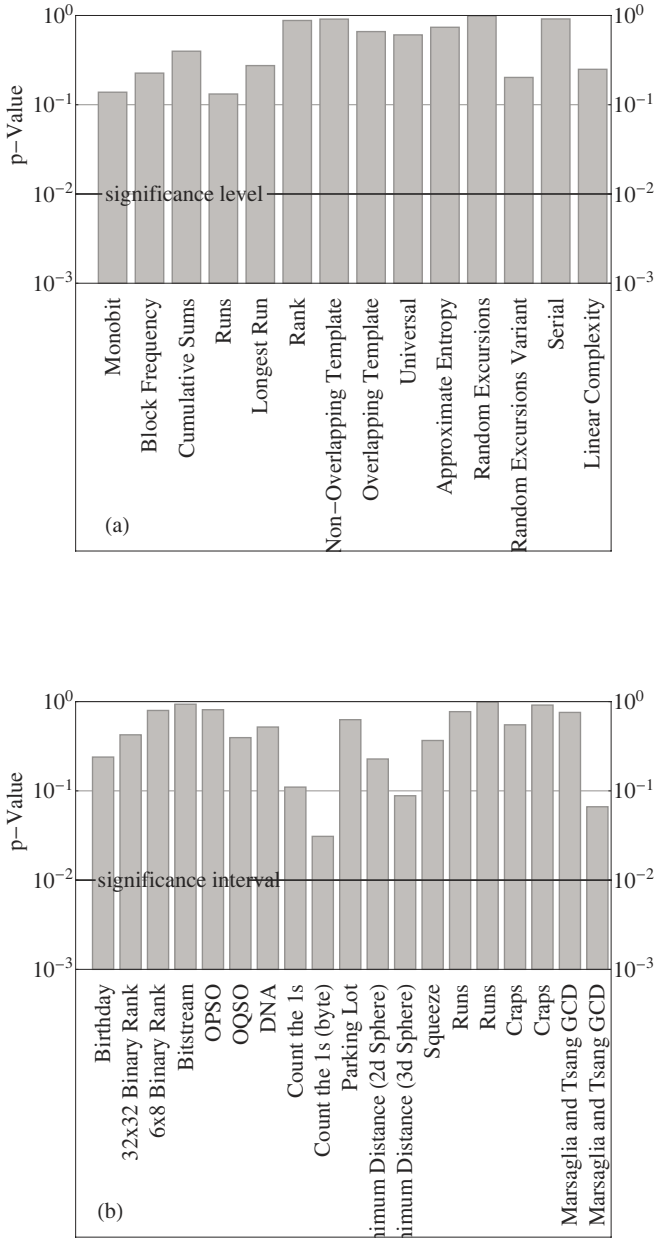

Fig. 5. Typical results of the standard statistical test suites STS (a) and Dieharder(b) for a typical sequence of 40 Gbit. Without processing, the p-values are routinely above the significance level confirming the quality and the reliability of the QRNG

#126957 - $15.00 USD Received 13 Apr 2010; revised 28 May 2010; accepted 1 Jun 2010; published 2 Jun 2010

4. Conclusion

In this contribution we have presented a ready-for-use random number generator, whose randomness directly originates from the randomness of quantum physics. Remarkably, the usually quite irksome dead time effects of a PMT turned out to be very positive for the performance of the QRNG. They significantly reduced the bias value of the random bits and enabled stable operation at very high rates. The implementation as a compact setup directly connected to a PC via a USB interface yielded a random bit-stream at a unprecedented rate of 50 Mbit/s, which was collected and analysed continuously over several days without any variation of the properties of the random bits observed. The random bit strings obtained routinely passed all the conventional test suites as well as on-the-fly monitoring. In particular, we could confirm the essential elements of a stochastic model for this QRNG and obtained pair correlations and the bias within the statistical limits. The system is easily scalable to even higher rates by simply implementing a multi-channel photomultiplier tube, thereby forming the ideal equipment for today's demanding applications such as numerical simulations, conventional cryptography, or novel, high rate quantum cryptography systems.

Acknowledgment

This work was supported by the BMBF project (QPENS).

#126957 - $15.00 USD Received 13 Apr 2010; revised 28 May 2010; accepted 1 Jun 2010; published 2 Jun 2010