Laser Physics Letters

LETTER

Quantum random number generator based on ‘Fermi–Dirac’ statistics of photocounts of faint laser pulses with a 75 Mbit s^{-1} rate

Laser Phys. Lett. **14** (2017) 125207 (6pp) https://doi.org/10.1088/1612-202X/aa930e

Letter

Quantum random number generator based on ‘Fermi–Dirac’ statistics of photocounts of faint laser pulses with a 75 Mbit s^{-1} rate

K A Balygin[1], V I Zaitsev[1], A N Klimov[1,2], S P Kulik[1], S N Molotkov[3,4,5], E Popova[6] and S Vinogradov[6,7]

[1] Faculty of Physics, M.V.Lomonosov State University, Moscow, Russia
[2] A.M.Prokhorov General Physics Institute RAS, Moscow, Russia
[3] Academy of Cryptography of Russian Federation, Moscow, Russia
[4] Institute of Solid State Physics, RAS, Chernogolovka, Moscow region, Russia
[5] Faculty of Computational Mathematics and Cybernetics, M.V. Lomonosov Moscow State University, Moskva, Russia
[6] National Research Nuclear University ‘MEPhI’, Moscow 115409, Russia
[7] P.N.Lebedev Physical Institute of the Russian Academy of Sciences, Moscow 119991, Russia

E-mail: sergei.molotkov@gmail.com

Received 3 October 2017
Accepted for publication 3 October 2017
Published 23 November 2017

Abstract

We implemented experimentally a quantum random number generator, based on the registration of quasi-single-photon light by a silicon photo-multiplier, which allows one to reliably achieve the Poisson statistics of photocounts. The use of the optimal grouping of photocounts and a polynomial-length sequence of the method for extracting the random sequence 0 and 1 made it possible to achieve the output rate of a provably random sequence up to 75 Mbit s^{-1}.

Keywords: quantum random number generator, quantum cryptography poisson statistics, photo-multiplier

(Some figures may appear in colour only in the online journal)

1. Introduction

A random number generator is the heart of any cryptographic system. In serious cryptographic systems based on symmetric encryption, only physical random number generators are used to generate the keys. The development of modern quantum technologies has opened new perspectives for the creation of a protected communication system. The most striking example is quantum cryptography. For the distribution of secret keys in systems of quantum cryptography, a large number of random sequences 0 and 1 are required. In particular, physical random number generators are used.

Physical random number generators can be divided into two types—classical and quantum. Physical classical random number generators are based on the extraction of randomness from some physical process, the evolution of which in time is described by the laws of classical physics. The evolution of any, even arbitrarily complex, classical system is described by differential equations. Sequences that are obtained at the output of such a generator are also not truly random, since they are completely determined by the initial conditions. Their randomness is related only to the uncertainty of the initial conditions for the system. Therefore, such generators can not be considered as truly random. The second type of physical generators is quantum (see, for example, the review [1] and references therein). The extraction of a random sequence of numbers is based on the measurements performed over quantum systems.

Unlike classical physics, measurements over a quantum system, each time prepared in a certain and the same state, produce an accidental result, which is the fundamental law of nature in the micro-world. Therefore, only random number generators can be truly random. A random sequence is a sequence of 0 and 1, which are independent in each position, and probability $P(0) = P(1) = \frac{1}{2}$.

The sequence of measurement results $(x_1, x_2, \dots x_n)$ over a quantum system in the general case is not statistically independent, i.e. the distribution function does not decompose into the product $P(x_1, x_2, \dots x_n) \neq P(x_1)P(x_2)\dots P(x_n)$. In this case, the number of truly random bits is given by min by the Renyi entropy $H_{\min} = -\log(\max_{P(x_1,x_2,\dots x_n)} P(x_1, x_2, \dots x_n))$. There are whole mathematical direction—randomness extractors, and there are procedures that allow one to extract randomness from the distribution $P(x_1, x_2, \dots x_n) \neq P(x_1)P(x_2)\dots P(x_n)$ (see, for example, [2]). However, the problem is that in a real situation, the distribution function $P(x_1, x_2, \dots x_n)$ is unknown. In addition, the very procedure of obtaining a truly random sequence requires a seed random sequence for randomly selecting a hash function.

It is convenient to choose such quantum-mechanical measurements that ensure the statistical independence of successive acts of measurement. It goes without saying that the verification of the correctness of the choice and the experimental realization of the physical process that ensures the statistical independence of the successive results of quantum mechanical measurements is checked at the final stage from the random sequence 0 and 1. This, however, takes place for both types of physical random number generators mentioned above.

Ideal quantum randomness might be the act of absorbing a single photon by an atom. Since a strictly single-photon source is currently absent, it is necessary to use quasi-single-photon states of light. In practice, such sources of quasi-single-photon states occur at the output of a strongly attenuated laser. The photon statistics of such light is supposed to be coherent.

As is known, the root cause of the Poisson statistics of photocounts while detecting laser radiation has a fundamentally quantum nature and is due to the absorption of photons by atoms (see details in [3]). The probability of finding m photons within a time window T at Poissonian statistics is (see for example, [3])

$$P_T(m) = \mathrm{e}^{-\mu}\frac{\mu^m}{m!}.$$

Since avalanche detectors do not distinguish the number of photons, random events are: either the absence of a photocount in the time slot (cycle) T—$\sqcup$ or photocount—$*$. In this case, the probability of photocounts (from one, two or more photons in the window T) is $P(*) = 1 - \mathrm{e}^{-\mu}$, respectively, the absence of a photocount is $P(\sqcup) = \mathrm{e}^{-\mu}$.

For the future it is important that the procedure for the extraction of randomness requires only statistical independence of photocounts and does not require knowledge of the probabilities themselves $p = P(\sqcup) 1 - p = P(*)$.

Strong attenuation is required to achieve statistical independence of the sequence of photocounts. This is due to the technical limitations of the avalanche detector's operation, more precisely due to the finite time of recovery of the detector after registration, which gives a limitation on the rate of formation of the random sequence. The rebuilding of the detector before the next registration act ensures the statistical independence of successive photocounts. Therefore, although they make it possible to achieve random sequences with good statistical properties, quantum random number generators are rather slow.

To achieve the maximum generation rate of random numbers, it is necessary to solve three main tasks.

(1) To choose a method for recording quasi-single-photon states of laser radiation, which ensures the statistical independence of photocounts.
(2) To choose a method of photocounts bunching, which provides extraction of all the randomness that is contained in the physical process.
(3) To choose a method of random extraction that allows algorithmically effective implementation.

2. Ideology in the implementation of QRNG

(1) The main problem in the photodetection of single-photon light by single-photon avalanche detectors (SPADs) [4] which operate in the Geiger mode is to take into account the dead time of the detector, which limits the clock frequency and the rate of photocounts. The clock frequency can not exceed the inverse time of the avalanche resolution. In addition, afterpulsing effects after recording a real photon can lead to parasitic counts after the registration of a photon. Both of these effects violate the ideal Poisson statistics of photocounts [5]. To eliminate these parasitic effects, no single SPADs were used, but instead the avalanche detector arrays contained several thousand such tiny SPADs connected in parallel silicon photo-multipliers (SiPMs) [6]. Since the average number of photons during a clock pulse does not exceed one thousand photons per pixel (see below), after registration with a separate photon detector, the probability that the next photon will fall into the same detector is extremely small. This allows one to increase the clock speed and the rate of photon input to the matrix. In this case, the dead time of a separate photodetector and the clock frequency are effectively unbound since the frequency band expands in a first approximation in proportion to the number of cells in the SiPM.
(2) In each time slot, there can be only a single photocount. All sequences of length n of cycles containing the same number of $\sqcup$ ($n - k$ levels—pieces) and $*$ (k particles) have the same probability. The number of such sequences is equal to the statistical weight for Fermi–Dirac statistics for the allocation of k fermions to $n - k$ levels [8]. As was shown earlier [9], such a natural bunching of sequences into classes with the same number $\sqcup$ and $*$ allows us to extract in the asymptotic limit all the randomness contained in the physical process.

(3) The extraction of all randomness reduces to the numbering of all equiprobable sequences from one class. We used an algorithm from the theory of arithmetic coding, which requires only polynomial memory resources along the length of the sequences. Direct table numbering requires an exponentially large memory 2^n, where n is the length of the sequence. The polynomial algorithm used allows processing sequences of 64 time slots. At this length, almost all randomness is extracted. Direct addressing would require $2^{64} \approx 10^{20}$ bits of memory, which is unrealistic.

3. Numbering sequences in classes and extracting a random sequence of 0 and 1

When extracting randomness, it is necessary to build a computationally efficient output block of the random sequence 0 and 1 from the sequence of photo-accounts of length n $i_1, i_2, \ldots i_n$ ($i_j = *$ or $\sqcup$). A tabular method of addressing this is possible when extracting a random sequence, which was used in our work [10]. The generation rate of random numbers with this method is technically limited by the size of the table, which grows exponentially along the length of the sequence.

Here we use the numbering method, which requires only polynomial resources along the length of the sequence, which allows us to process practically sequences of any length. It is convenient to use methods and results from the theory of arithmetic coding. The extraction of randomness occurs in two stages.

At the first stage the output sequence $i_1, i_2, \ldots i_n$, is given by the number, which is determined by the polynomial algorithm (see details in [11]). Suppose that there are K counts in the sequence *. Denote the position number by the index j_m. Then, there is a one-to-one correspondence between the sequence of photocounts $(i_1, i_2, \ldots i_n)$ and its number $\mathrm{Num}(i_1, i_2, \ldots i_n)$ $(0 \leqslant \mathrm{Num}(i_1, i_2, \ldots i_n) \leqslant C_n^K - 1)$

$$\mathrm{Num}(i_1, i_2, \ldots i_n) = C^1_{j_1-1} + C^2_{j_2-1} + \ldots + C^k_{j_k-1}, \quad C^l_j = 0, \quad j < l. \tag{1}$$

Binomial coefficients can be calculated in advance and placed in a table of size $n \times n$. The binomial coefficient is selected on the fly as soon as the photocounts $(^*)$ appear. When the first count appears at position j_1, a number (binomial coefficient) is selected at the intersection of the first line j_1 of the row and the first column of the matrix. When the second count appears, the coefficient in the matrix is taken at the intersection of j_2 of the row and the second column, etc. The result is the sequence number $\mathrm{Num}(i_1, i_2, \ldots i_n)$. The method of numbering the sequences of photocounts from the class is explained in figure 1(a)). Let the sequence belong to some class, the total number of sequences in the class N_k.

The second step is to obtain a block of random 0 and 1 from the sequence number. Sequence numbers are in the range $0 \leqslant \mathrm{Num} \leqslant N_k - 1$. Let the number of the current sequence be Num.

Then the procedure is recursively executed. If the number of the current sequence Num is in the interval $2^{k_0} + 2^{k_1} + \ldots + 2^{k_{i-1}} \leqslant \mathrm{Num} \leqslant 2^{k_0} + 2^{k_1} + \ldots + 2^{k_{i-1}} + 2^{k_i} - 1$, $(i \leqslant i_{\max})$, then the output random sequence is k_i lower order bits of the binary representation Num. The number of sequence numbers in this range is 2^{k_i}.

For example, $N_k = 6 = (110)_2$, let the sequence number $\mathrm{Num} = 3 = (011)_2$, then the output is (11). If $\mathrm{Num} = 5 = (101)_2$, then one gets (01) at output.

4. Physical realization QRNG

The functional diagram of QRNG is shown in figure 1(b)). The scheme uses the minimum number of elements.

The SiPMs used have been developed by MEPhI-Pulsar (Moscow, Russia) and produced by the Technological Center of MIET (Zelenograd, Russia). The SiPMs have a sensitive area approx 1×1 mm^2 and consisted of $N_{\text{pix}} = 1156$ pixels with 32×32 μ^2. The operational voltage (several volts above breakdown) is 40V [7]. The temperature of the detector was stabilized at 25^0 C. The source of radiation was a LED (SLD3143VL) from a Sony Laser Diode with a working wavelength of 0.405 μ. For processing we used FPGA of Intel FPGA (Altera) at 150 MHz frequency. Also, we used an external interface USB 2.0 for outputting a resultant random sequence in a continuous regime. The advantage of the SiPMs that we use for registering the light is their high value of the quenching resistors R_q, which exceeds 1 MOhm. Due to this fact the SiPMs possess quite low afterpulsing probability since the dead time after firing the pixel is proportional to R_q ($t = R_q \cdot C_p$, where C_p is the pixel capacitance). During the pixel recovery process, for which duration is determined by the dead time, for the most part the charge carriers released from the traps produced in the primary discharge do not have the ability to initiate correlated discharge in that pixel. Another very important feature of such an SiPM is the quite fast and narrow pixel signal, which is of the order of 1 ns for a very simple readout by using only 2 output pins (in contrast to the fast output of the Sensl SiPMs which requires 3 pins for the connection).

It should be noted that requirements to the SiPM parameters gained, for example, from the cryptography applications, are not the same as for the conventional mass market, which is mostly governed now by medical applications (Positron Emission Thomography (PET) and time-of-flight TOF PET). This means that special development of SiPMs devoted to very important strategic application areas is mandatory in order to obtain the highest possible quality and safety of Quantum Random Number Generators.

5. The average number of photons per pixel

Let us estimate the average number of photons incident on an individual pixel. This estimate is important to be sure that the generator is really quantum, and indeed photocounts from quasi-one-photon radiation are actually recorded. Let us verify that the generator actually works in the quantum mode. To do this we need to estimate the average number of photons incident on the SiPM. The actual observed value

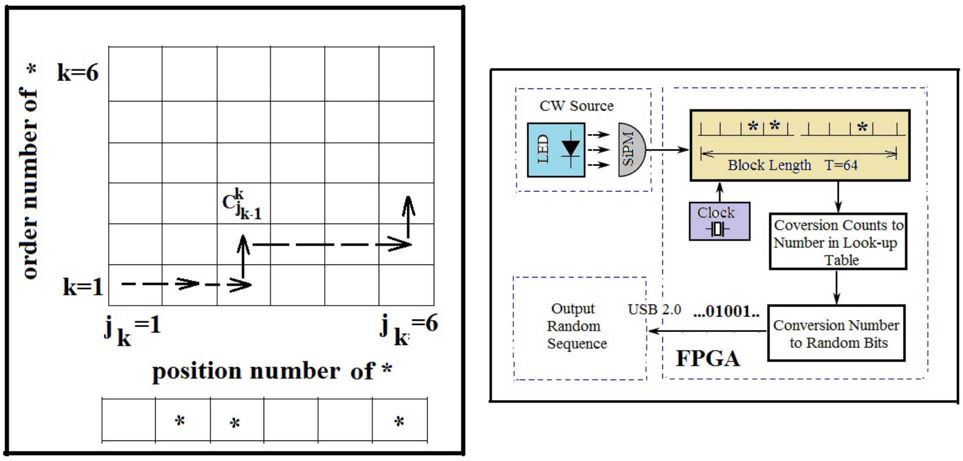

Figure 1. (a) Let us consider the example of sequence numbering of photocounts. Here, the length of the sequence is 6. The binomial coefficients in the table are computed once in advance. The horizontal dashed arrows indicate movement along the table as the sequence appears in the bar from left to right. Counting number 1 appears on bar 2, then the binomial coefficient in the table is taken, which is the vertical solid arrow. Then move horizontally in the table until the next report appears. Counting number 2 appears in measure number 3, the horizontal shaded arrow to the third measure—the row in the table. Then the solid arrow up to the second horizontal row—the number of the series is the reference number of the reference. Then move horizontally until the next countdown appears in step number 6 (the dashed arrow), the reference number 3. Then follow the solid arrow to the horizontal at number 3. In this case, at each step the binomial coefficients in the corresponding positions of the table are summed. The sum is the sequence number of the sequence in the class. Recall that the class is determined by the number of photocounts. (b) Functional block diagram of a random number generator. The clock rate was 150 MHz. The pulse duration at half-height is less than 2 ns.

is the probability of counting for one time slot (clock cycle) $P(*) = 0.255$. This probability is equal to $P(*) = \mu \cdot N_{\text{pix}}$, μ is the average number of photons per pixel in the SiPM per time slot, $N_{\text{pix}} = 1156$ is the number of pixels in the matrix. Finally we get $\mu = \frac{P(*)}{N_{\text{pix}}} \approx 0.221 \cdot 10^{-3}$ (average number of photons per sample per pixel), i.e. one pixel accepts less than a hundredth of a photon. For a coherent state with Poisson statistics, the probability to find a single photon $P(n = 1) = \mathrm{e}^{-\mu}\mu \approx \mu$ ($\mu \ll 1$), respectively, the probability to find pair of photons is $P(n = 2) = \mathrm{e}^{-\mu}\frac{\mu^2}{2} \approx 0.244 \cdot 10^{-7}$. Thus, a single-photon case is almost realized.

It is important to note that in order to take into account the possible parasitic effect of the cross-talk effect between neighboring pixels on the statistics of photocounts (see, for example, [12]), additional research was carried out. At our working levels of photon fluxes, there was no distortion of the statistics (see figure 2).

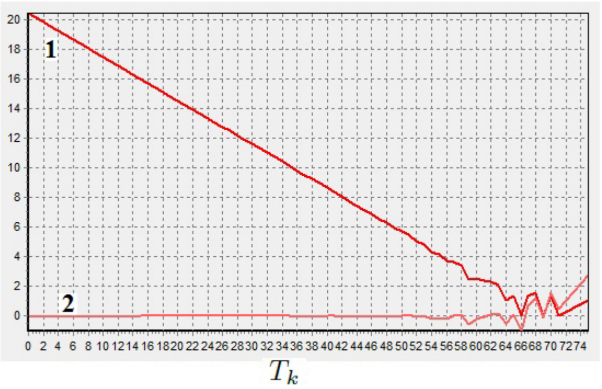

Figure 2. Curve 1 $(\ln(\Sigma(T_k)))$ is the logarithm of the numbers of cycles between the successive registration times T_k, k is the number of cycles. Labels on the abscissa axis correspond to the number of cycles at a frequency of f = 150 MHz. Curve 2 is the logarithm of the number of time intervals with subtraction of the slope. The observed probability of counting for one time slot is $P(*) = 0.255$. Recall that the theoretical limit of the speed of generation of random numbers is $f \cdot h(P(*)) = 122.85$ MHz, $h(x) = -x\log(x) - (1 - x)\log(1 - x)$—binary entropy function. The histogram was built with accumulation, the total number of events in the histogram $\sum_{k=0}^{128}\Sigma(T_k) = 290\,444\,0341$. The number of counts in the first histogram box 740 566 410, respectively, is $\ln(740\,566\,410) = 20.423$. At the upper limit of the duration of intervals of 128 cycles, the probability of counts is practically zero. Fluctuations in the time interval between samples with the number of cycles >70 are associated with rare events due to the exponential dependence of the time interval distribution function. The length of the processed blocks to extract random blocks was selected in 64 cycles.

6. Demonstration of Poisson statistics of photocounts

The use of SiPM detectors makes it possible to achieve near-ideal Poisson statistics of photocounts. In the case of Poisson statistics, the intervals between consecutive samples are a random quantity that obeys the geometric distribution

$$P(T_k) = (1 - P(*))^{k-1}P(*), \tag{2}$$

here T_k is the number of cycles between successive registration times. For ideal Poisson statistics, the logarithm of the probability $\ln(P(T_k))$ (k is the number of cycles) should be a linear dependence on k. Figure 2 shows the experimental histogram. As follows from figure 2, the dependence shows Poisson statistics. With a large distance between photocounts, the probability of events is small, so deviations from the line in figure 2 with a distance of more than 70 cycles between successive photocounts are associated with a low probability

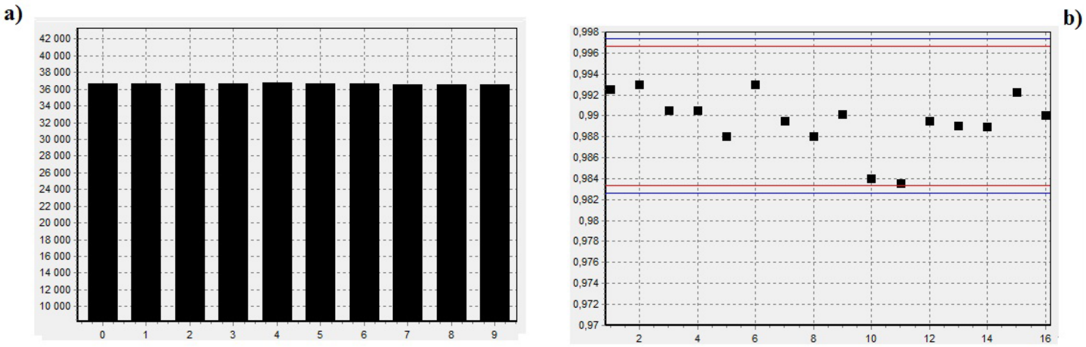

Figure 3. (a) A histogram of the values ν_j (P-value) for all tests falling into 10 intervals $j = 0, ...9$. Interval [0.0.0.1] corresponds to the value $j = 0$ along the abscissa. The value $j = 1$ corresponds to the interval $[0.1, 0.2]$ along the abscissa, etc. The histogram was constructed for 2000 random sequences $4 \cdot 10^6$ bit each. (b) The y-axis is the proportion of sequences that passed the tests for the values of P-value. On the abscissa axis, the numbers correspond to different tests for the NIST nomenclature [14]. The red horizontal lines show the upper and lower bounds ('three sigma') according to all tests except the *12—Random Excursions Test* and *13—Random Excursions Variant Test*. For these two tests, the number of test sequences N is not defined in advance, but is determined in the testing process. The upper and lower bounds ('three sigma') for these two tests are shown by the blue horizontal lines. For the remaining tests, the number of test sequences is $N = 2000$ each with a length of $4 \cdot 10^6$ bits.

of such events. The latter means that the length of the processed sequences $n = 64$ can guarantee the Poisson character of the statistics of photocounts.

7. The generation rate of a random sequence and checking its statistical properties

The achieved generation rate of the resulting random sequence 0 and 1 was 75 Mbit s^{-1}. Recently we have demonstrated that the technique discussed above allows one to build a quantum random number generator achieving 64 Mbit s^{-1} [13]. Here we siginficanly improve both the registration procedure and data statistical development. Moreover, we exploited an advanced SiPM developed by MEPhI-Pulsar (Moscow, Russia).

To check the statistical properties of random sequences, the standard set of NIST tests was selected [14]. The hypothesis H_0 is checked, or in other words, we check whether the given sequence is truly random. If this is so, then the various statistics of the S or groups 0 and 1 are also random variables; the probability distributions of various statistics with the length of the sequence $n \to \infty$ should tend to some standard distributions for the random sequence. Then we specify a certain significance level for α and a certain threshold for each statistic. If the probability of deviating the statistics exceeds the threshold value, then the hypothesis of randomness is rejected, the sequence is discarded. This means that even a generator of ideal random sequences can give out a sequence that has such an evasion.

Next, the probability P-value is calculated. It is the probability that even an ideal random source can produce a sequence with such a deviation of statistics. If $P > \alpha$, then the hypothesis H_0 is accepted, for $P < \alpha$, the hypothesis is rejected, the sequence is not considered to be random.

Interpretation of P-value—values. Given the significance level of α, P-value, there is a possibility that even an ideal generator 'has the right' to generate with such probability a sequence that will appear to be not random for this test. The smaller the P-value, the less likely the ideal generator is 'entitled' to generate such a sequence. If the calculated P-value is greater than α, then the test is considered passed. The standard value of significance level for $\alpha \in [0.001, 0.01]$ [14]. We used $\alpha = 0.01$. The proportion of the sequences that passed the tests is itself a random variable. The allowable range of fluctuations is determined by the variance of the P-value. P-values are random variables with a Bernoulli distribution with two outcomes. One—the test is passed, the second outcome—the test is not passed. The allowable spread of P-values should fit into 'three sigma'. The variance for a P-value is $P(1 - P)N$ (N is the number of test sequences). According to [14], at a significance level of $\alpha = 0.01$, all P-values should fall within the interval 'three sigma' $1 - P \pm 3\sqrt{\frac{P(1-P)}{N}} = 0.99 \pm \frac{0.297}{N}$. A test for the uniformity of the values of the P-value. With a large number of tested sequences, the total value of the P-value for all tests is a sum of identically distributed quantities that is distributed according to the Gaussian normal law [10]. In this case, statistics $X_N^2 = \sum_{j=1}^{M} \frac{(\nu_j - N \cdot p_j)^2}{N \cdot p_j}$, where ν_j is the fraction of P-value values falling into the jth interval [0, 1], p_j is the true probability of falling into the jth interval. With a large number of test sequences, the probability distribution of X_N^2 does not depend on the distribution p_j and tends to the Pearson distribution $\chi^2(N - 1)$ with $(N - 1)$th degree of freedom [15]. The recommended number of intervals is $M = 10$ [14]. The threshold value for the null hypothesis (H_0 is a random sequence) of the admissible spread is obtained for a given significance level α from the relation $\Pr\{X_N^2 > t_\alpha | H_0\} = \alpha$, where $t_\alpha = \chi^2_{1-\alpha,N-1}$—$(1 - \alpha)$th quantile of the distribution χ^2 with $(N - 1)$ th degree of freedom. In other words, if the evasion of statistics $X_N^2 > \chi^2_{1-\alpha,N-1}$, then the null hypothesis H_0 is rejected, and the sequence is not accidental. The deviation of statistics from the allowable rate (for a given probability-level of significance) is exceeded. Uniformity test P-value is considered passed if P-value from P-value

$\hat{P} = \frac{\int_{\chi^2_K}^{\infty} \mathrm{d}x \mathrm{e}^{-x/2} x^{K/2-1}}{2^{K/2}\Gamma(K/2)}, \quad K = N - 1,$ not less than $\hat{P} > 0.0001$, the homogeneity test is considered passed, and a H_0 hypothesis is adopted.

Figure 3 shows the results of the uniformity test of P-value (figure 3(a))). The value of P-value from P-value is equal to $\hat{P} > 0.997\,852\,53$, which must be greater than the critical $\hat{P}_c > 0.0001$. The test for the uniformity of P-value with a margin passed. The proportion of the sequences that passed the test is shown in figure 3(b)) for all tests (the NIST test numbers [14] are shown horizontally). For all tests, the proportion of sequences that passed tests for P-value lies within 'three sigma', which means a successful passing of tests—the hypothesis of randomness of the sequence is accepted.

Acknowledgment

We express our gratitude to colleagues from the Academy of Cryptography of the Russian Federation for their discussions and support. The authors also thank I M Arbekov, I V Radchenko and K S Kravtsov for helpful discussions. The work of K A Balygin, V I Zaitsev, A N Klimov and S N Molotkov was supported by the Russian Science Foundation (project no. 16-12-00015). This work for E Popova and S Vinogradov was supported by Russian grants # 3.2989.2017/4.6 and 3.8484.2017/9.10/.

References

[1] Herrero-Collantes M and Carlos Garcia-Escartin J 2017 Quantum random number generators *Rev. Mod. Phys.* **89** 015004

[2] König R, Renner R and Schaffner C 2009 The operational meaning of min- and max-entropy *IEEE Trans. Inf. Theory* **55** 4337

[3] Klyshko D N 1988 *Photons and Nonlinear Optics* (New York: Gordon and Breach)
Klyshko D N and Masalov A V 1995 Photon noise: observation, squeezing, interpretation *Phys.—Usp.* **38** 1203

[4] Bronzi D, Villa F, Tisa S, Tosi A and Zappa F 2016 SPAD figures of merit for photon-counting, photon-timing, and imaging applications: a review *IEEE Sensors J.* **16** 3

[5] Vinogradov S 2012 Analytical models of probability distribution and excess noise factor of solid state photomultiplier signals with crosstalk *Nucl. Instrum. Methods Phys. Res.* A **695** 247

[6] Danilov M (representing the CALICE Collaboration) 2007 Scintillator tile hadron calorimeter with novel SiPM readout *Nucl. Instrum. Methods* A **582** 451

[7] Buzhan P *et al* 2006 Large area silicon photomultipliers: performance and applications *Nucl. Instrum. Methods Phys. Res.* A **567** 78

[8] Landau L D and Lifshits E M 1980 *Statistical Physics* 3rd edn, Part I (Oxford: Butterworth-Heinemann)

[9] Molotkov S N 2017 On the limiting characteristics of quantum random number generators at various clusterings of photocounts *JETP Lett.* **105** 395

[10] Kravtsov K S, Radchenko I V, Kulik S P and Molotkov S N 2015 Minimalist design of a robust real-time quantum random number generator *J. Opt. Soc. Am.* **32** 1743

[11] Babkin V F 1971 A universal encoding method with nonexponential work expenditure for a source of independent messages *Probl. Inf. Trans.* **7** 288

[12] Kalashnikov D A, Tan S-H and Krivitsky L A 2012 Crosstalk calibration of multi-pixel photon counters using coherent states *Opt. Express* **20** 5044

[13] Balygin K A, Zaitsev V I, Klimov A N, Kulik S P and Molotkov S N 2017 The implementation of a quantum random number generator based on the optimal grouping of photocounts *JETP Lett.* **106** 451 (in Russian)

[14] Bassham L *et al* 2010 A statistical test suite for the validation of random number generators and pseudo random number generators for cryptographic applications *NIST SP 800-22rev1a* (https://csrc.nist.gov/Projects/Random-Bit-Generation/Documentation-and-Software)

[15] Cramer H 1946 *Mathematical Methods of Statistics* (Princeton, NJ: Princeton University Press)