

Minimalist design of a robust real-time quantum random number generator

K. S. KRAVTSOV,^{1,2,*} I. V. RADCHENKO,^{1,2} S. P. KULIK,¹ AND S. N. MOLOTKOV^{3,4,5}

¹Faculty of Physics, Moscow State University, Moscow, Russia

²A.M. Prokhorov General Physics Institute RAS, Moscow, Russia

³Academy of Cryptography of Russian Federation, Moscow, Russia

⁴Institute of Solid State Physics, Chernogolovka, Moscow Region, Russia

⁵Faculty of Computational Mathematics and Cybernetics, Moscow State University, Moscow, Russia

*Corresponding author: kravtsov@kapella.gpi.ru

Received 16 March 2015; revised 6 July 2015; accepted 6 July 2015; posted 7 July 2015 (Doc. ID 236343); published 28 July 2015

We present a simple and robust construction of a real-time quantum random number generator. Our minimalist approach ensures stable operation of the device as well as its simple and straightforward hardware implementation as a stand-alone module. As a source of randomness the device uses measurements of time intervals between clicks of a single-photon detector. The obtained raw sequence is then filtered and processed by a deterministic randomness extractor, which is realized as a look-up table. This enables high-speed on-the-fly processing without the need of extensive computations. The overall performance of the device is around 1 random bit per detector click, resulting in 1.2 Mbit/s generation rate in our implementation. © 2015 Optical Society of America

OCIS codes: (270.5290) Photon statistics; (270.5568) Quantum cryptography.

<http://dx.doi.org/10.1364/JOSAB.32.001743>

Random number generation has attracted a lot of attention since quantum technologies became available to serve this purpose. Quantum random number generation gives access to the universal randomness of quantum mechanics, which is unavailable, at least theoretically, in classical physics. Over the last 20 years there has been a number of different quantum random number generator (QRNG) approaches and suggestions about its practical implementation. In the present work we looked for a highly practical and easy way to implement QRNG, which will ensure stable operation due to its overall simplicity. To keep it simple we intentionally considered only designs with one single-photon detector (SPD). Along with the physical part, not less important was the choice of a randomness extraction algorithm, which, by itself, should guarantee generation of independent and unbiased bits at the output under any conditions.

There are many different approaches to quantum randomness generation described in the literature [1–11]. Still, it is hard to clearly distinguish between what we call “quantum” and what in some sense belongs to statistical physics. We associate the former with the use of simple “quantum measurements” and SPDs (or other particles), and believe that most other methods belong to the latter case, where it is harder to explain why the source is truly unpredictable and thus whether it can in principle generate true randomness. Among the SPD-based sources it is highly beneficial to use

a single SPD in the whole setup. Besides the obvious reliability advantage, it also eliminates the need of any hardware calibration as SPDs typically have a large variation of performance parameters even within a particular type. Using more than one SPD also does not give an advantage in the generation rate: typically the result is the same as the corresponding multiple of single SPD devices.

The output of an SPD contains only timing information (it could also be a number of photons, but conventional SPDs do not resolve it), i.e., moments when a particular photon caused an avalanche in the detector. This is the only data available for random numbers extraction. Realization of a quantum measurement may require engineered light pulses, for example in a “which way” experiment [3], or in a “multiple choice” one [12], but from the standpoint of performance those settings are suboptimal: instead of using any time moment measurable by the clock, we intentionally limit ourselves to only a few or several of them. Thus, in this sense the optimal design should use a continuously running light source.

The simplest form of this method is detection of the arrival times of photons from a cw coherent source [1,5,6,9,11]. This gives purely Poissonian statistics, which are simple to work with. A modification with a temporally shaped cw source is also possible [13] and gives slightly better performance at the expense of an increased system complexity and reduced reliability, which is unsuitable for our concept.

Collecting timing information is commonly done in two different forms: timestamping arriving photons by the value of a free-running clock counter as in [1,5,11,14], or counting the number of clock cycles between adjacent detection events [6,9]. The two are completely identical by the amount of obtained information (each form of data can be easily converted to the other one), but the second form consists of independent integers, while the first one unavoidably contains internal correlations. The correlations come from the slowly changing most significant bits of the time counter. A direct calculation [1] shows that in order to make correlations negligible, one has to ensure that bit values change some 15 times faster than the average counting rate, which poses a significant limitation on the amount of random data obtained. Thus, storing time intervals between detector clicks is advantageous as, by the definition of the Poisson process, all such values are perfectly independent. They are distributed with the exponential distribution, favoring small numbers and exponentially decaying toward the large ones.

Another not less important aspect of this approach is light generation. In principle, it would be the best to use a single (transverse, temporal, and polarization) mode cw coherent light source. In practice, however, it is not possible. We use instead an alternative approach, based on mode averaging. Even if the statistic of a single mode is not necessarily Poissonian, the more modes we detect, the closer the output will resemble Poissonian process due to the Palm–Khintchine theorem [15]. Thus, a substantially multimode detection allows us to arrive at a Poissonian process regardless of the photon statistic in each of the modes.

After a raw stream of random data is acquired one needs to process it in order to obtain random and independent bits. This processing, or extraction, can be done in many different ways with two global approaches: using deterministic algorithms and with seeded extractors. The second approach is much more powerful as it is capable of extracting randomness from any type of a partially random sequence; however, in this work we stick to the first one. Seeded extractors need a perfectly random seed to operate. Until recently such algorithms required more random bits than they produced, e.g., using Toeplitz matrices [11]. Later, a new Trevisan extractors family [16] was introduced, which allows for generating more randomness than was consumed as the seed. It also allows reusing the seed for future conversions [17].

The main difficulty with seeded extractors is that they are constructed for a particular rate of min-entropy provided by the source. After it is defined the extractor gives a certain rate of compression, which does not depend on anything, including the actual quality of the raw sequence. This creates a possible flaw in the system: if for any reason the raw sequence degrades, the output of the seeded extractor will cease to be truly random. Such algorithms intrinsically lack any adaptivity and may easily fail with a temporal drift of experimental parameters affecting the amount of generated entropy.

Other problems include estimation of min-entropy of the source and real-time realization of such an extractor, especially Trevisan. Strictly speaking, it is impossible to measure min-entropy of any given source in finite time. Knowing the internal structure of the source helps but does not make the problem

trivial. At the same time this parameter remains the only parameter that defines whether the QRNG output is random or not. It may become even more critical with reusing the extractor output as the seed. Real-time processing is rather a technical but nevertheless one more important issue. Recent results show that realization of Trevisan construction with modern computers yields some 17 kbits/s output bit rate [18]. Apparently, this is orders of magnitude slower than the entropy generation rate by a typical SPD. Such a computational-hungry algorithm is hard to run when the system performance is not ignored.

Based on the given discussion, we think that deterministic algorithms, if applicable, are better suited for our goals. Here we should notice that a popular approach [6,8,13] of using standard hash functions such as SHA-256 is, strictly speaking, invalid [9] as it does not extract randomness, but rather only compresses the raw data in some peculiar fashion. It does not guarantee independence of output bits and possesses similar weaknesses as seeded extractors. Talking about deterministic extractors, one needs to know properties of the input data. As was shown earlier we consider a stream of positive and independent integers with the exponential probability distribution. The goal of the extractor is to convert this stream into unbiased and independent bits.

The most trivial but inefficient method is to convert the stream into independent but biased bits by taking the integers modulo 2 and then eliminate the bias using the von Neumann algorithm [19]. We use a generalization of this method to a finite alphabet of $M > 2$ letters—the extended Elias algorithm [20], which is asymptotically efficient, converging to the entropy of the source (see also [21]). Importantly, here any deterministic conversion of the obtained positive integers into the finite alphabet may be used, as it does not affect the quality of the extractor output. It is desirable, however, to approach the uniform probability distribution within the alphabet to decrease the entropy loss.

Realization of the Elias extraction algorithm is explicitly given in [22]. Briefly, the input sequence is cut into words of N letters each. A probability of getting a particular word is exactly the same as for all the words, which are permutations of letters of the original one. The total number of such permutations gives the number of equiprobable states, one of which is obtained as the original word. All such states can be numbered, and the number of the one obtained can be converted into random bits using its binary representation.

An example of extraction for $M = N = 4$ is shown in Fig. 1. The strings AAAA, ..., DDDD are mapped onto the empty set because they all have different probabilities of appearance unless the probability of obtaining the individual letters A, B, C, and D is exactly equal. The patterns ABBB, BABB, BBAB, and BBBA, and the like, generate two output bits because if the letter-generating events are independent, each combination of letters has four equiprobable permutations irrespective of the probability of obtaining the individual letters A, ..., D. The largest number of permutations is obtained for the word ABCD, giving 24 variants; each results in 3 or 4 output bits.

Following our minimalist doctrine we wanted to simplify required processing as much as possible. Taking into account

(4,0,0,0)	(3,1,0,0)	(2,2,0,0)	(2,1,1,0)	(1,1,1,1)
AAAA → ∅	BBBC → 00	AACC → 00	ABBD → 000	ABCD → 0000
	BBCB → 01	ACAC → 01	ABDB → 001	ABDC → 0001
	BCBB → 10	ACCA → 10	... → → ...
	CBBB → 11	CAAC → 11	BDAB → 111	CBDA → 1111
		CACA → 0	BDBA → 00	CDAB → 000
		CCAA → 1	DABB → 01	CDBA → 001
			DBAB → 10	... → ...
			DBBA → 11	DCBA → 111
$f = 4/256$	$f = 48/256$	$f = 36/256$	$f = 144/256$	$f = 24/256$

Fig. 1. Extraction of random bits for $M = N = 4$. The first line shows a word pattern, i.e., a sorted list of repetition numbers of each letter. The corresponding extraction process is given below on the example of one permutation family. The value f shows the share of a particular pattern in all $M^N = 256$ possible input words; it coincides with the actual frequency of appearance if all letters are equiprobable.

that the expected throughput of the extractor should be in Mbits/s range, we sacrificed the efficiency of extraction but made it suitable for realization as a look-up table in a standard memory chip. In our implementation we use an alphabet of $M = 4$ letters and make conversions using blocks of $N = 10$ such values. This matches the 20-bit address space of the 2 MB flash memory chip used. Another limitation that favors smaller alphabets and shorter processing blocks is the requirement of the process to be stationary: if parameters of the process drift, the output sequence may not be random anymore. The process must be stationary during the time required to run through all possible combinations within a processing block, whose number is of the order of M^N . Thus, a substantial increase of the alphabet size and the block length will also require a guarantee of stability not for seconds, but for hours and even days, which is almost impossible to guarantee in practice. Any feedback loop in the system, e.g., for keeping the constant count rate, should be substantially slower than this time, rendering the system to be extremely slow and impractical.

Figure 2 shows the simulated efficiency of the extraction algorithm for a varying size of the binary buffer $b = N \lceil \log M \rceil$ needed to store the whole processing block. The

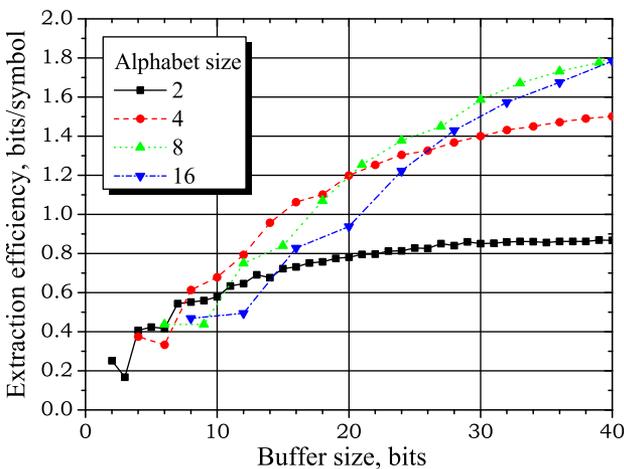


Fig. 2. Extraction efficiency of the implemented algorithm versus the size of the buffer for different alphabet sizes. The actual generator uses a 20-bit buffer and a four-symbol alphabet, yielding 1.2 bits per raw symbol.

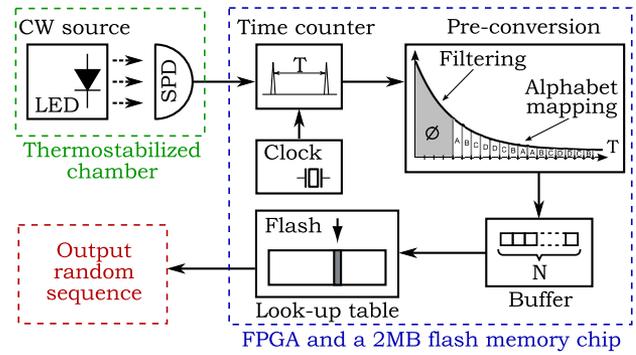


Fig. 3. Block diagram of the experimental setup.

data are calculated for a uniform distribution of the input symbols and contain traces for different alphabet sizes M , which are conveniently chosen as the powers of 2. One can see that for a chosen pair of $M = 4$ and $N = 10$ the algorithm generates 1.2 bits per input symbol. It is easy to note that scaling with the memory size is rather poor: even for a 40-bit address space, which is unrealistic and raises temporal stability concerns, the efficiency only approaches 1.8 bits per symbol. Thus, even as we sacrificed the bit generation rate for system simplicity and better output quality, we are still not too far from potential limits of this scheme.

The discussed principles and ideas were fulfilled in our experimental realization (see Fig. 3) based on a silicon SPD with a thin depletion layer and a $\varnothing 30 \mu\text{m}$ sensitive area. All processing is made in a field-programmable gate array (FPGA) attached to a 2 MB flash memory chip. A red LED ($\lambda \approx 627 \text{ nm}$, spectral width $\Delta\lambda \approx 45 \text{ nm}$) driven with a $\approx 10 \mu\text{A}$ current is used as a light source, while the whole pair of the LED and the SPD is temperature stabilized at $+25^\circ\text{C}$. A feedback loop is used for stabilization of the count rate by adjustment of the LED current. The last one has a time constant of 16 s to ensure that the process is stationary on the time scale of M^N counts.

A major flaw in the experimental system with respect to the theory is nonideal characteristics of the SPD. For the presented QRNG structure it is, first of all, temporal parameters of the SPD. While the photon arrival process is the Poissonian one, the generation of SPD clicks is not. It has a highly suppressed probability of detection right after the previous click, known as a dead time. It may also have the opposite effect with another temporal shape called afterpulsing, i.e., triggering further detector clicks by a previous one even when no other photons are present.

Our study of the actual process was performed at the same average count rate as used in the final device, namely 1.2 MHz. Figure 4 shows count frequency histogram as a function of a delay between successive clicks. It ideally fits the expected exponential distribution except for the intervals shorter than 150 ns. A deviation from the expected distribution fits well by an exponential decay function with the time constant of 40 ns.

Whatever is the nature of these nonidealities, as long as we can measure the maximal time period which is still affected, we can easily filter out dependent events by making sure that not a

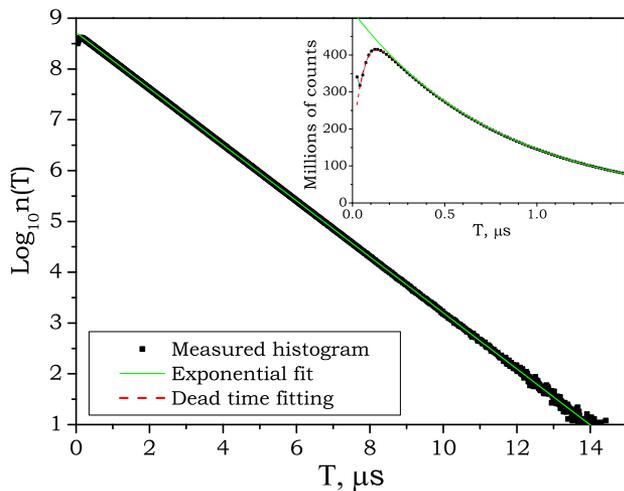


Fig. 4. Measured histogram of waiting times between detector clicks at the average rate of 1.2×10^6 clicks/s. A pronounced deviation from the expected exponential behavior is seen at $T \lesssim 150$ ns.

single time interval shorter than the specified time is used for random number generation. In general, we model the real SPD as an ideal detector giving Poissonian statistics, with a perturbation function with a maximal memory of τ . To get rid of dependent events we use a simple digital filter that rejects all time intervals shorter than 160 ns, reducing the events rate from 1.2 to 1.0 MHz.

Another significant flaw of the actual system is the presence of dark counts. The dark count rate of the detector used is around 200 Hz, which is almost 4 orders of magnitude smaller than the regular count rate. Although the nature of dark counts is much more complicated and not obviously as “quantum” as photodetection events, it still has nearly Poissonian statistics and does not affect any obtained results. We can only say that 0.01% of the generated entropy may not be enough “quantum.”

The detector clicks are time tagged with a resolution of 16 ns and corresponding time intervals are calculated. All intervals shorter than 160 ns are discarded, while the remaining ones are converted into a four-symbol alphabet, as shown in Fig. 5. The particular conversion scheme gives a more uniform distribution than the trivial modulo operation. Blocks of 10 successive symbols represented as ten 2-bit strings form a 20-bit address in the memory chip pointing to a 2-byte precalculated value. The number of output bits varies depending on the symbols obtained from zero (when all 10 symbols are the same) to 14 bits (the maximum number of permutations is $10!/(3!3!2!2!) = 25200$). To enable this variable size output, a simple binary coding is used when the actual output data is left-padded with 1 and zeroes to form a 16-bit string $0\dots 01ab\dots yz$, where k is the output string size and $ab\dots yz$ is the string itself.

Generated random bit sequences were characterized using the NIST statistical test suite. Testing 1 Gbit consecutive data chunks with $\alpha = 0.01$ using 1000 bit streams by 10^6 bits showed the pass ratio well above 0.98 for all tests. The

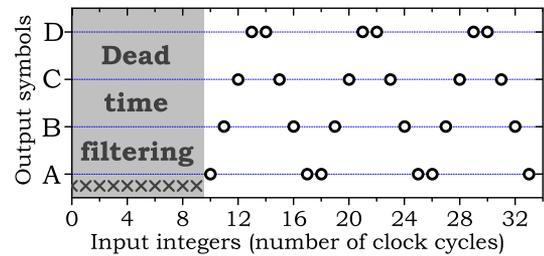


Fig. 5. Conversion of digitized time intervals into a four-letter alphabet with bias reduction via bidirectional coding and a time filter cutoff of 10 clock cycles.

P -value $_T$ of the uniformity chi-square test among P -values obtained for each stream is 0.68, which is above the 0.0001 confidence level. All obtained results suggest that generated sequences are indistinguishable from truly random ones by the particular tests. The broad scope of the NIST suite and clear implemented QRNG operation principles confirm that the generated random data are of high quality and may be used in critical applications.

In conclusion, we have experimentally demonstrated a quantum random number generator based on the measurement of waiting times in the process of photon arrival at the SPD. The main concept of the device is its simplicity, robustness, and real-time operation. The used deterministic randomness extractor together with a straightforward raw data processing enables adaptive random bits extraction that guarantees output quality regardless of the actual entropy of the source.

Funding. Government Future Research Fund (FPI).

REFERENCES

1. C. H. Vincent, “The generation of truly random binary numbers,” *J. Phys. E* **3**, 594–598 (1970).
2. T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, “A fast and compact quantum random number generator,” *Rev. Sci. Instrum.* **71**, 1675–1680 (2000).
3. A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, “Optical quantum random number generator,” *J. Mod. Opt.* **47**, 595–598 (2000).
4. M. Fiorentino, C. Santori, S. M. Spillane, R. G. Beausoleil, and W. J. Munro, “Secure self-calibrating quantum random-bit generator,” *Phys. Rev. A* **75**, 032334 (2007).
5. 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).
6. M. A. Wayne, E. R. Jeffrey, G. M. Akselrod, and P. G. Kwiat, “Photon arrival time quantum random number generation,” *J. Mod. Opt.* **56**, 516–522 (2009).
7. I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, “An optical ultrafast random bit generator,” *Nat. Photonics* **4**, 58–61 (2010).
8. C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, “A generator for unique quantum random numbers based on vacuum states,” *Nat. Photonics* **4**, 711–715 (2010).
9. 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.* **98**, 171105 (2011).

10. B. Sanguinetti, A. Martin, H. Zbinden, and N. Gisin, "Quantum random number generation on a mobile phone," *Phys. Rev. X* **4**, 031056 (2014).
11. Y.-Q. Nie, H.-F. Zhang, Z. Zhang, J. Wang, X. Ma, J. Zhang, and J.-W. Pan, "Practical and fast quantum random number generation based on photon arrival time relative to external reference," *Appl. Phys. Lett.* **104**, 051110 (2014).
12. N. Lutkenhaus, J. L. Cohen, and H.-K. Lo, "Efficient use of detectors for random number generation," U.S. patent 7,197,523 (March 27, 2007).
13. M. A. Wayne and P. G. Kwiat, "Low-bias high-speed quantum random number generator via shaped optical pulses," *Opt. Express* **18**, 9351–9357 (2010).
14. M. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, "High speed optical quantum random number generation," *Opt. Express* **18**, 13029–13037 (2010).
15. D. P. Heyman and M. J. Sobel, "Superposition of renewal processes," in *Stochastic Models in Operations Research: Stochastic Processes and Operating Characteristics* (Dover, 2004), p. 158, Chap. 5.8.
16. L. Trevisan, "Extractors and pseudorandom generators," *J. ACM* **48**, 860–879 (2001).
17. X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, "Post-processing for quantum random-number generators: entropy evaluation and randomness extraction," *Phys. Rev. A* **87**, 062327 (2013).
18. W. Mauerer, C. Portmann, and V. B. Scholz, "A modular framework for randomness extraction based on Trevisan's construction," arXiv:1212.0520 (2012).
19. J. von Neumann, "Various techniques used in connection with random digits," in *Monte Carlo Method*, Vol. 12 of Applied Mathematics Series (U.S. National Bureau of Standards, 1951), pp. 36–38.
20. P. Elias, "The efficient construction of an unbiased random sequence," *Ann. Math. Stat.* **43**, 865–870 (1972).
21. Y. Peres, "Iterating von Neumann's procedure for extracting random bits," *Ann. Stat.* **20**, 590–597 (1992).
22. A. Juels, M. Jakobsson, E. Shriver, and B. K. Hillyer, "How to turn loaded dice into fair coins," *IEEE Trans. Inf. Theory* **46**, 911–921 (2000).