K. S. Kravtsov, S. P. Kulik, I. V. Radchenko, Quantum random number generator, *Mat. Vopr. Kriptogr.*, 2016, Volume 7, Issue 2, 111–114

DOI: 10.4213/mvk188

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2016 Т. 7 № 2 С. 111–114

УДК 519.254.1+53.082.7

Quantum random number generator

K. S. Kravtsov, S. P. Kulik, I. V. Radchenko

Lomonosov Moscow State University, Moscow

Получено 18.II.2015

Abstract. A quantum random number generator (QRNG) based on a photoeffect as a true random process was proposed and implemented as a stand-alone module. It uses a deterministic post-processing algorithm to overcome physical imperfections of real components. Our minimalistic design of QRNG prevents possible loopholes and makes it suitable for commercial production. The proposed QRNG provides a binary output stream of 1.2 Mbit/s that successfully passes NIST statistical tests.

Keywords: random number generation, quantum random number generator, randomness extractor

Квантовый генератор случайных чисел

К. С. Кравцов, С. П. Кулик, И. В. Радченко

Московский государственный университет имени М. В. Ломоносова, Москва

Аннотация. Описан квантовый генератор случайных чисел (КГСЧ), основанный на истинно случайном процессе фотоэффекта, реализованный в виде отдельного модуля. Для устранения физических нерегулярностей компонент используется детерминистический алгоритм дополнительной обработки получаемых случайных чисел. Наша минималистская схема КГСЧ защищает от возможных утечек информации и пригодна для коммерческого использования. Предлагаемый КГСЧ порождает двоичную выходную последовательность с частотой 1.2 Мбит/сек, которая успешно проходит батарею статистических тестов НИСТ.

Ключевые слова: генераторы случайных чисел, квантовый генератор случайных чисел, случайные числа, извлечение случайности

Citation: *Mathematical Aspects of Cryptography*, 2016, v. 7, № 2, pp. 111–114 (Russian)

A random number generator (RNG) is a critical component of almost all modern key distribution systems (either classical or quantum), some examples of exceptions are given by protocols having the randomization as an implicit property of the key distribution scheme by itself (Ekert-like protocols [1]). Any RNG controlled by the only classical physics laws suffers from its deterministic description and, therefore, theoretical possibility of output stream prediction, while a quantum random number generator (QRNG) is supplied by a physical process of a quantum nature, which is natively random. At the moment, a large number of approaches to QRNG has been proposed and implemented [2–5], but the nomenclature of commercially available devices remains negligible. The necessity of reliable and replicable QRNG construction has motivated the creation of the proposed QRNG.

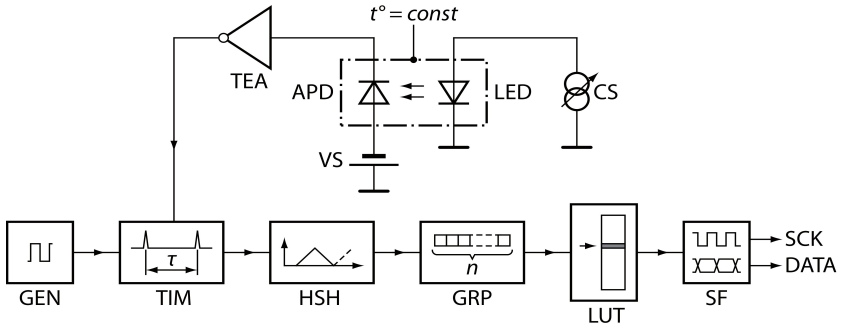

Fig. 1. Block diagram of QRNG. LED — light emitting diode, APD — avalanche photo diode, CS and VS — current and voltage sources, TEA — transimpedance amplifier, GEN — clock generator, TIM — time interval measurement, HSH — hash function — randomness extractor, GRP — group letters in words, LUT — look-up table, SF — binary stream forming

The base of our QRNG is a photoeffect process in an avalanche photo diode stimulated by a non-coherent electromagnetic field. A light emitting diode (LED) and a thin depletion layer metal-resistor-semiconductor avalanche photodiode (APD) are mounted opposite of each other on the same axis (Fig. 1). The electrical current flowing through the LED and, thus, the emitted light are so weak that the APD works in the Geiger mode. Time intervals between the clicks of the detector measured with a discrete time scale by the TIM constitute a raw sequence used for random number generation. The temperature of the LED and APD is held constant to stabilize their parameters. The LED current is controlled by a feedback loop to maintain a constant average APD count rate of 1.2 Mcps regardless of the spread and drift of actual setup parameters.

The time bin for interval measurements is $T = 20$ ns while the typical line width of the LED is 40 nm with a center wavelength of 630 nm, which gives a coherence time of $\tau_{coh} \sim 10^{-15}$ s $\ll T$.

It moves us towards a multimode detection regime, where the detector cannot feel the field statistics, so the action of light upon the APD is the same as for a classical field. Under these assumptions, a photoionization process is essentially quantum and therefore truly-random. The Mandel's formula [8] in this case predicts a Poisson statistics of the APD clicks and the exponential decay for the time-between-clicks distribution. However, due to the limitations of real components, the experimental distribution appears to be distorted. The deviations observed can be fully explained by the effects of a dark-time and an after-pulsing in a real APD [7]. The mismatch leads to the presence of non-zero correlations between the adjacent time intervals in the sequence, which are effectively suppressed by a modulo-like hash function — randomness extractor:

$$H(\tau) = \begin{cases} \varnothing, & \tau < s, \\ (\tau - s) \bmod m, & \tau \geqslant s, (\tau - s) \bmod (2m) < m, \\ m - 1 - (\tau - s) \bmod m, & \tau \geqslant s, (\tau - s) \bmod (2m) \geqslant m, \end{cases} \quad (1)$$

If a time interval τ is shorter than s, it is rejected to weaken the influence of an after-pulsing effect; otherwise the interval is fed through a non-monotonic hash function. The value of $T \cdot s$ should be greater than APD dead-time and after-pulsing period; m should be much less than mean click period $\langle\tau\rangle$. The particular form of the extractor was chosen for reasons of practical implementation simplicity and ensures 3 aims:

- to map semi-infinite set of time intervals to a finite number of letters in the output alphabet,
- to extract randomness from the initial sequence, and
- to make the distribution of letters more uniform.

The extractor (1) doesn't equalize probabilities of letters m perfectly, but it makes the sequential algorithm more efficient.

We suppose that the letter sequences are non-correlated and stationary. To equalize outcome probabilities we use the Elias algorithm for $m \geqslant 2$ letters in $n \geqslant 2$ positions [6]. The letter sequence is cut into blocks or words of m elements each by the GRP. The words are then divided into classes containing words with the same set of letters appearing in different orders, so all words in each class obviously have the same probability. By numbering words in each class we obtain equiprobable output values. Our knowledge of the cardinality of a class the word belongs to and the word number in this class allows us to convert the sequence of words into the output binary stream.

To avoid time-consuming computations our prototype implements the Elias algorithm via a pre-calculated look-up table (LUT) held in a 2 MiByte FLASH ROM. The parameters $s = 8$, $m = 4$ and $n = 10$ have been chosen to yield the average value of 1.0 output bit per APD click.

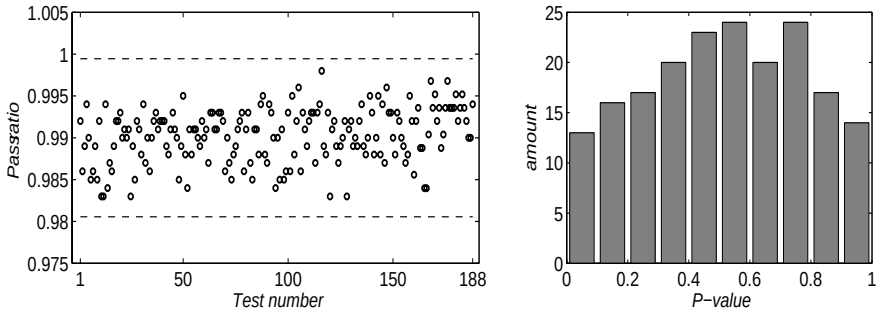

Fig. 2. NIST statistical test suite results. On the left: portion of sequences passing a test, confidence interval is marked by dash lines. On the right: distribution of P-values

The output of the QRNG was tested by NIST statistical test suite [9] with the parameter $\alpha = 0.01$, upon 1000 streams of 10^6 bits. The results are presented in Fig. 2. All samples of the sequence passing the tests are inside the confidence interval, while the P-value distribution has parameters $\chi^2 = 7.7$; $P_{\text{value}\,T} = 0.68 > 0.0001$, which suggests that the generated sequence is indistinguishable from a truly random one by the particular tests. The broad scope of the NIST suite and clear implemented QRNG operation principles guarantee that the generated random data are of high quality and may be used in critical applications.

Список литературы

[1] Ekert A. K., "Quantum cryptography based on Bell's theorem", *Phys. Rev. Lett.*, **67**:6 (1991), 661–663.

[2] Jennewein T., Achleitner U., Weihs G., Weinfurter H., Zeilinger A., "A fast and compact quantum random number generator", *Rev. Sci. Instrum.*, **71**:4 (2000), 1675–1680.

[3] Wayne M. A., Jeffrey E. R., Akselrod G. M., Kwiat P. G., "Photon arrival time quantum random number generation", *J. Mod. Opt.*, **56**:4 (2009), 516–522.

[4] Wahl M., Leifgen M., Berlin M., Röhlicke T., Rahn H.-J., Benson O., "An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements", *Appl. Phys. Lett.*, **98**:17 (2011), 171105.

[5] Wayne M. A., Kwiat P. G., "Low-bias high-speed quantum random number generator via shaped optical pulses", *Opt. Express*, **18**:9 (2010), 9351–9357.

[6] Juels A. Jakobsson M., Shriver E., Hillyer B. K., "How to turn loaded dice into fair coins", *IEEE Trans. Inf. Theory*, **IT-46**:3 (2000), 911–921.

[7] Cova S., Ghioni M., Lacaita A., Samori C., Zappa F., "Avalanche photodiodes and quenching circuits for single-photon detection", *Appl. Opt.*, **35**:12 (1996), 1956–1976.

[8] Mandel L., "Fluctuations of photon beams: The distribution of photo-electrons", *Proc. Phys. Soc.*, **74**:3 (1959), 233–242.

[9] *Random Number Generation. NIST statistical test suite*, Gaithersburg, MD: NIST, http://csrc.nist.gov/groups/ST/toolkit/rng/index.html.