# INSTRUMENTAL AND MATHEMATICAL METHODS IN MANAGEMENT PROCESSES

## Polarisation-optical model of a controlled random number generator

Received 10.11.2021 Revised 01.12.2021 Accepted 07.12.2021

UDC 004.383.4 JEL O31 DOI https://doi.org/10.26425/2658-3445-2021-4-4-47-54

**Aleksei V. Glazkov**

Lecturer, State University of Management, Moscow, Russia

ORCID: 0000-0003-2796-7054

*e-mail: av_glazkov@guu.ru*

**Irina K. Dzhioeva**

Cand. Sci. (Econ.), Assoc. Prof., South Ossetian State University, Tskhinval, Republic of South Ossetia

ORCID: 0000-0002-3352-8608

*e-mail: djioeva_irina@mail.ru*

**Dmitrii V. Pervukhin**

Senior Lecturer, State University of Management, Moscow, Russia

ORCID: 0000-0001-6500-035X

*e-mail: dv_pervuhin@guu.ru*

**Anna A. Pruchkina**

Cand. Sci. (Phys. and Math.), Senior Researcher, P.N. Lebedev Physical Institute of the Russian Academy of Sciences, Moscow, Russia

ORCID: M-7550-2015

*e-mail: pruchkina_aa@mail.ru*

**Georgy O. Rytikov**

CEO, LLC "Impact Electronics", Moscow, Russia

ORCID: 0000-0001-5521-8662

*e-mail: gr-yandex@yandex.ru*

### ABSTRACT

The subject of the paper is an original model of a tunable optical random number generator. The purpose of the article is to analyse the possibilities of using the proposed model to ensure the protection of the control signals in the projected telecommunication management system of the robotised agro-industrial complex of the Republic of South Ossetia.

The research was carried out by methods of mathematical and information-logical modeling. The main results of the study are the information-logical model of the hardware implementation prototype, the descriptive mathematical model of its functioning and the obtained dependences of the quantitative characteristics of the generated random numbers statistical distributions on the main control parameter of the experimental setup.

These results can be used in the design and the operation of the remote production facilities monitoring and management telecommunication systems' components. The possibilities of prototype creating and functioning were demonstrated by visualising the schematic chart of the experimental equipment and by the quantitative estimates of "one" and "zero" signals observation probabilities under the different polarisation rotator orientations relative to the plane of the optical signals detecting system.

### KEYWORDS

Digital transformation risks, information security, optoinformatics, random number generator, laser, polarisation, statistical distribution, South Ossetia

### FOR CITATION

Glazkov A.V., Dzhioeva I.K., Pervukhin D.V., Pruchkina A.A., Rytikov G.O. (2021) Polarisation-optical model of a controlled random number generator. *E-Management*, vol. 4, no. 4, pp. 47–54. DOI: 10.26425/2658-3445-2021-4-4-47-54

### ACKNOWLEDGEMENTS

The reported study was funded by RFBR and MES RSO, project number 21-51-00001.

# ИНСТРУМЕНТАЛЬНЫЕ И МАТЕМАТИЧЕСКИЕ МЕТОДЫ В ПРОЦЕССАХ УПРАВЛЕНИЯ

## Поляризационно-оптическая модель управляемого генератора случайных чисел

Получено 10.11.2021 Доработано после рецензирования 01.12.2021 Принято 07.12.2021

УДК 004.383.4

**Глазков Алексей Владимирович**
Преподаватель, ФГБОУ ВО «Государственный университет управления», г. Москва, Российская Федерация
ORCID: 0000-0003-2796-7054
*e-mail: av_glazkov@guu.ru*

**Джиоева Ирина Константиновна**
Канд. экон. наук, доц., ГАОУ «Юго-Осетинский государственный университет им. А.А. Тибилова», г. Цхинвал, Республика Южная Осетия
ORCID: 0000-0002-3352-8608
*e-mail: djioeva_irina@mail.ru*

**Первухин Дмитрий Васильевич**
Ст. преподаватель, ФГБОУ ВО «Государственный университет управления», г. Москва, Российская Федерация
ORCID: 0000-0001-6500-035X
*e-mail: dv_pervuhin@guu.ru*

**Пручкина Анна Артемовна**
Канд. физ.-мат. наук, ст. науч. сотрудник, ФГБУН «Физический институт им. П.Н. Лебедева Российской академии наук», г. Москва, Российская Федерация
ORCID: M-7550-2015
*e-mail: pruchkina_aa@mail.ru*

**Рытиков Георгий Олегович**
Ген. директор, ООО «Импакт Электроникс», г. Москва, Российская Федерация
ORCID: 0000-0001-5521-8662
*e-mail: gr-yandex@yandex.ru*

### АННОТАЦИЯ

Предметом исследования представленной научной работы является оригинальная модель настраиваемого оптического генератора случайных чисел. Цель статьи – анализ возможностей использования предложенной модели с целью обеспечения защиты управляющих сигналов в проектируемой системе телекоммуникационного управления роботизированным агропромышленным комплексом в Республике Южная Осетия.

В исследовании использовались методы математического и информационно-логического моделирования. Основными результатами исследования являются создание информационно-логической модели прототипа аппаратной реализации, описательной математической модели его функционирования и полученные зависимости количественных характеристик статистических распределений генерируемых случайных чисел от основного управляющего параметра экспериментальной установки.

Полученные результаты могут использоваться в процессе проектирования и эксплуатации компонентов телекоммуникационных систем мониторинга и управления удаленными производственными объектами. Возможности создания и функционирования прототипа данных систем продемонстрированы визуализацией принципиальной схемы экспериментального оборудования и количественными оценками вероятностей наблюдения сигналов «один» и «ноль» при различных ориентациях поляризационного ротатора относительно плоскости системы детектирования оптических сигналов.

### КЛЮЧЕВЫЕ СЛОВА

Риски цифровой трансформации, информационная безопасность, оптоинформатика, генератор случайных чисел, лазер, поляризация, статистическое распределение, Южная Осетия

### ДЛЯ ЦИТИРОВАНИЯ

Глазков А.В., Джиоева И.К., Первухин Д.В., Пручкина А.А., Рытиков Г.О. Поляризационно-оптическая модель управляемого генератора случайных чисел//E-Management. 2021. Т. 4, № 4. С. 47–54.

### БЛАГОДАРНОСТИ

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 21-51-00001.

## INTRODUCTION

### Motivation

The issues of reliable security of the information and communication processes and systems are receiving the increasing attention with the beginning of the global campaign for comprehensive computerisation and digitalisation of industrial and social-economy spheres all over the world [Alcácer, Cruz-Machado, 2019; Frolova et al., 2018; Kamolov, 2017]. The unique economic conditions have developed in the Republic of South Ossetia as a result of a number of well-known historical and political processes. They allow to form (not "to rebuild") the high-tech sectors in main segments of the region economy. But the additional risks of high degree informatisation in industry and agriculture should be taken into account [Djioeva et al., 2019; Dzhioeva et al., 2018; Dzhioeva & Tehov, 2017]. We propose to use the encryption of control signals using a two-component digital key formed by the developed model of a controlled optical random number generator as a reliable way to increase the degree of information protection in the designed specialised telecommunication networks intended for the remote control of the robotised agricultural production [Rytikov, 2007; Morozova et al., 2014; Iskhakov et al., 2008].

### Review

The random (and pseudo-random) numbers are those that can be considered as the realisation of some random variable. We usually mean the realisations of a random variable uniformly distributed over the interval (0,1). A random number can be defined as a set of random digits. And a random digit in the n-digit number system is the result of an abstract experiment with n equally probable outcomes (each of the outcomes corresponds to one of the n digits). Such experiments are assumed to be statistically independent [Soshnikov, 2000; Breiman, 2011; Noh & Rieger, 2004].

The random numbers are used as auxiliary elements in the implementation of some algorithms in computing. In cryptography, they are used when generating secret messages as a key body or as the elements that allow key calculating. In some cases (for example, in computational algorithms such as the Monte-Carlo techniques), it is sufficient to use pseudorandom numbers. Pseudorandom numbers, unlike random ones, form a sequence, each subsequent member of which can be calculated if the previous ones are known. But, in cryptography, it is important that each subsequent random number is as little as possible related to the previous ones. However, the use of pseudorandom numbers is also practically possible if the calculating of the next member of a sequence of numbers is associated with the insurmountable computational difficulties [Hastings 1970; Binder, 1997; Sobol, 1998; Sobol, Levitan, 1998; Maaranen et al., 2004; Barash & Shchur, 2011; Vadhan, 2011].

Let's suppose that it is necessary to generate a sequence of 1024 random bits. Assuming that 8 bits are enough for binary encoding of one character, we get that with the help of such a key it is possible to encode a text with a length of about 100 characters. Such "telegraphic" messages can be used both for transmitting information from a distributed system of sensors and detectors to server equipment and for transferring the control signals to the actuators [Yang et al., 1998; Liu et al., 2002; Yu et al., 2017].

The direct interception of one such message does not allow an attacker to establish either the content of the message or the nature of the statistical distribution of generated random numbers. However, the interception of a series of such messages already makes it possible to determine with some probability the functional characteristics of the random number generator (RNG), since the parameters of the statistical probability distribution of observing zeros and ones are determined precisely by the properties of the RNG and not by the features of the message language. Consequently, the use of random number generators characterised by stationary statistical distributions with fixed parameters makes it possible for an attacker to gradually obtain and accumulate additional information about the control system. Ultimately, he can, based on the studied statistics, begin to generate meaningless or even false malicious control signals that will either disable the production system or force it to function with technology violations, as a result of which the manufactured products will acquire a poorly predictable list of negative properties for the end user. Thus, in order to ensure the reliability of the transmitted control signals, it is necessary that the distribution changes every time, and the sender and the addressee at any given time must have the same implementations of a dynamically changing random key [Nyberg, 1994; Boneh & Lipton, 1996; Baptista, 1998; Foulkes et al., 2001; Gisin et al., 2002; Kim & Lebedev, 2004; Myasnikov & Roman'Kov, 2015].

At the moment, there is quite a large number of prototypes of physical random number generators and an incalculable number of implementations of computational pseudo-random number generators. Both have their own advantages and disadvantages. Various computational methods are used to generate pseudorandom numbers. Their main disadvantage for cryptographic applications is actually pseudo-randomness. Their main advantage is the convenience of managing distribution parameters which is initially embedded in the computational algorithms [Phillips et al., 2011; Demchik, 2011; Barash & Shchur, 2014].

To synthesise a sequence of random digits the classical and the quantum random number generators are often used. The classical generators use classical physical processes, for example, electronic device noise or thermal noise. Therefore, in principle, they are advanced pseudo-random number generators. Although the current level of computer technology development does not allow to describe the dynamics of such processes in a deterministic way, nevertheless, in principle, the classical processes are recognised as deterministic, and, therefore, are not truly random. In addition, in contrast to pseudo-random number generators, it is difficult or fundamentally impossible to control the distribution parameters for classical random number generators [Fill, 1998; Srinivasan et al., 2003; Manssen et al., 2012].

The quantum generators of truly random numbers use quantum physical processes, for example, the decay of radioactive elements or the probabilistic nature of the interaction of a photon with a beam splitter. Such processes are recognised as "truly random" and not subject to complete determination as satisfying the Heisenberg uncertainty relation. It is also quite difficult to control the distribution parameters for quantum generators of truly random numbers [Steane, 1998; Jennewein et al., 2000; Fürst et al., 2010].

We propose to combine the best qualities of random and pseudorandom number generators. It is necessary to modify the type of generators of truly random numbers in such a way that the parameters of the probability distribution obtained as a result of the generator operation can vary within certain limits at the request of the system user.

## MAIN SECTION

### Theory and methods

Let's form a mathematical model that characterises a random number generator. Consider a random number with a length of N binary registers. Denote $p_i$ the probability that the digit "0" will is written in the $i$-th register of the random number. Then $q_i = (1 - p_i)$ is the probability of the digit "1" is written in this register. By the way, we can call "pseudorandom" those numbers for which the probability $p_i = F\ (i, p_{i-1}, p_{i-2}, \dots)$ depends at least on the register number and may also depend on the values that are written in previous registers. The probability $p_i$ for the "truly" random numbers is a constant: $p_i = p = const$.

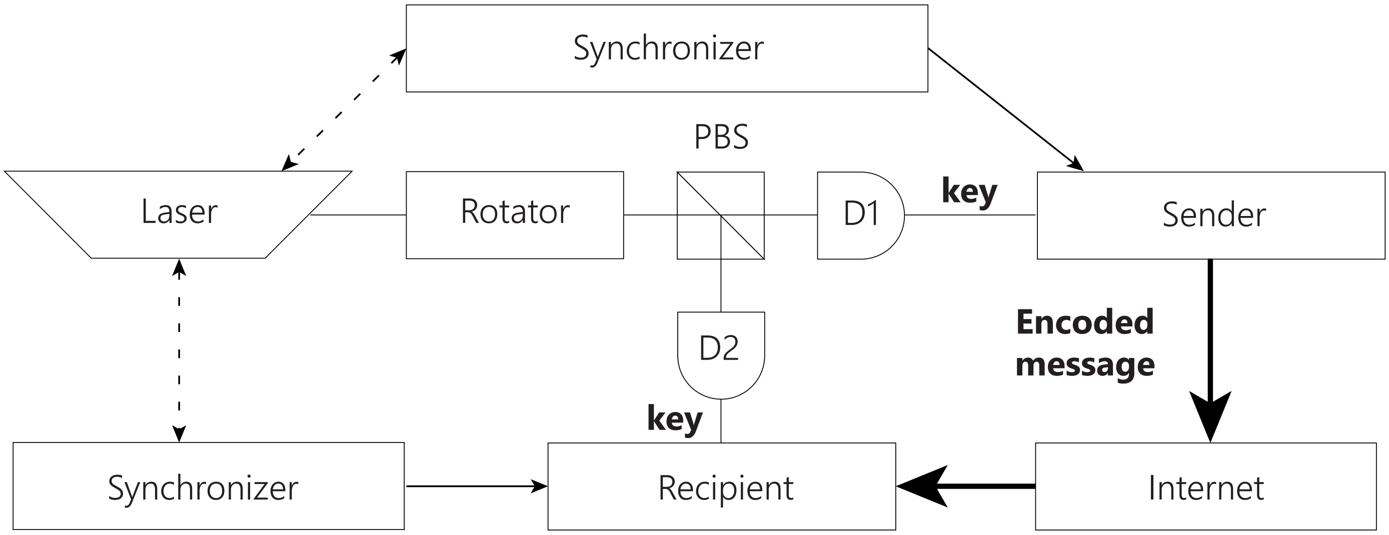
It is obvious that the probability of observing zeros and ones in the binary number under consideration will be described by a binomial distribution [Hartley & Fitch, 1951; Tarone, 1979; Wood et al., 2016]:

$$P(k) = C_k^N p^k q^{N-k} = C_k^N p^k (1-p)^{N-k}. \tag{1}$$

Thus, by changing only one parameter (the probability of observing a random digit), it is possible to control the main parameters (maximum value and width) of the entire probability distribution that characterise the random number generator.

Now let's form an information-logical model of a prototype of an experimental setup allowing the exchange of secret messages and using an optical random number generator to dynamically create a secret key (see figure 1).

Under the optical implementation of the information processes it is convenient to encode "zeros" and "ones" by the polarisation state of light pulses of the coherent (laser) light. If the polarisation plane of linearly polarised laser light coincides with one of the proper (so-called "basis") directions of the polarisation beam splitter (PBS), then almost all photons will fall into only one detector (for example, D1). So the probability of observing one type of random digits will be close to one, and the distribution (1) will take the form of the Dirac function with a) a width determined by the degree of linearity of the polarisation of the incident light and the quality of the polarisation beam splitter and b) a height determined by the requirements of the normalisation and the information-logical meaning of the "probability" concept:



rotator is an optical element that rotates the plane of light polarisation; PBS – polarisation beam splitter; D1, D2 – detectors

*Compiled by the authors on the materials of the study*

**Figure 1.** An experimental setup diagram that allows the secret messages exchanging using an optical random number generator to create a secret key

$$P_1(k) = C_k^N 1^k 0^{N-k} = \delta(N). \tag{2}$$

If the plane of the coherent light polarisation is oriented at the angle of π/4 to the basic directions of PBS, then, since each photon truly randomly ($p_i = p = 0{,}5$) “chooses” the direction in which it “passes” through the beam splitter, the distribution takes the form:

$$P_{0,5}(k) = C_k^N 0{,}5^k 0{,}5^{N-k} = C_k^N 0{,}5^N. \tag{3}$$

Thus, by changing the angle of rotation of the plane of the coherent light polarisation relative to the intrinsic basis of the polarisation beam splitter, it is possible to influence the parameters of probability distributions that characterise the optoinformatic devices under consideration.

The sender and the recipient must first get a shared secret key to transmit a secret message. The corresponding measurements of the photocurrent in the detectors are made at the time points set by the synchroniser. In case of weak light fields (about one photon per measurement time) the measurement results of the receiver and sender are anticorrelated. Thus, for N measurements, the participants of the information exchange get two chains of random binary digits anticorrelated with each other. One of the participants inverts the received random number, as a result of which the identical secret key is formed. The elimination of the information losses caused by photon absorption in optical paths can be achieved through the use of error correction protocols. Next, the information is encoded and the encoded message is forwarded via an Internet-type channel.

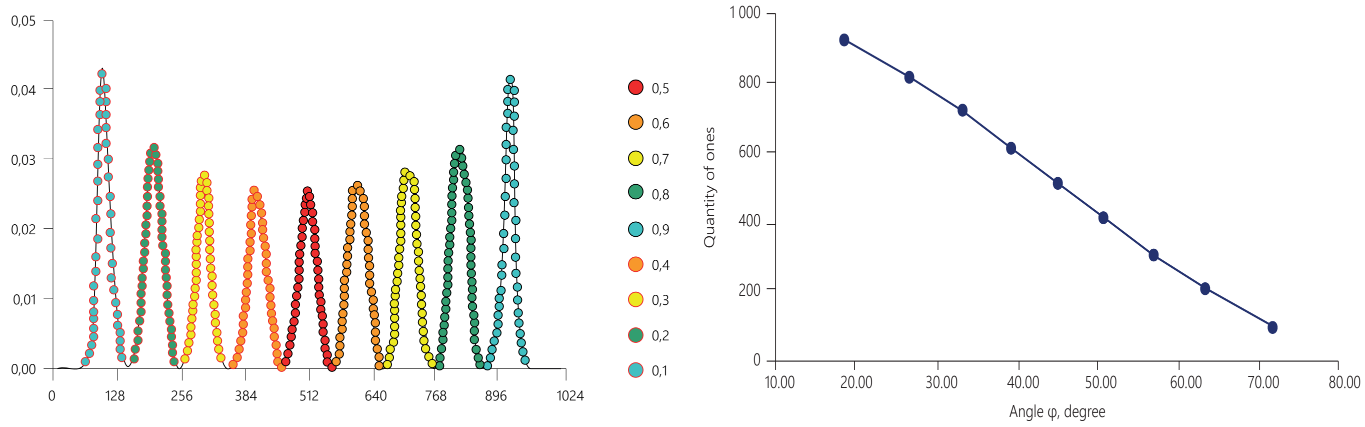
## RESULTS AND DISCUSSION

In in the general case the distribution takes the form:

$$P(k) = C_k^N \cdot (\cos\varphi)^{2k} \cdot (\sin\varphi)^{2(N-k)}, \tag{4}$$

where φ is the angle between the light polarisation plane and one of the axes of the proper basis of the polarisation beam splitter.

Figure 2 shows the distributions of the number of units in a message of 1024 bits at different values of the probability of “one”-observing.



*a*) binomial distributions at different values of probabilities of detecting one (zero)

*b*) dependences of observing quantity of ones (zeros) on the rotation angle of the rotator

*Compiled by the authors on the materials of the study*

**Figure 2.** The distributions of the number of units in a message of 1024 bits at different values of the probability of "one"-observing

It is possible to set a "floating" distribution of the number of "ones" and "zeros" turning the rotator in an arbitrary way (using a classical pseudorandom number generator).

## CONCLUSION

It seems likely that the above model of a tunable random number generator can find some application even in quantum computer science and quantum cryptography. For example, some algorithms of "quantum hacking" use the so-called "oracle", the implementation of which can be a random number generator. "Tunability" will allow analogically selecting distribution forms that correspond to specific implementations of random number generators used by participants in the process of secret information exchanging.

## REFERENCES

Alcácer V. and Cruz-Machado V. (2019), "Scanning the industry 4.0: a literature review on technologies for manufacturing systems", *Engineering Science and Technology an International Journal*, vol. 22, no. 3, pp. 899–919. https://doi.org/10.1016/j.jestch.2019.01.006

Baptista M.S. (1998), "Cryptography with chaos", *Physics Letters A*, vol. 240, no. 1-2, pp. 50–54. https://dx.doi.org/10.1016/S0375-9601(98)00086-3

Barash L.Yu. and Shchur L.N. (2014), "PRAND: GPU accelerated parallel random number generation library: using most reliable algorithms and applying parallelism of modern GPUs and CPUs", *Computer Physics Communications*, vol. 185, no. 4, pp. 1343–1353. https://doi.org/10.1016/j.cpc.2014.01.007

Barash L.Yu. and Shchur L.N. (2011), "RNGSSELIB: program library for random number generation, SSE2 realization", *Computer Physics Communications*, vol. 182, no. 7, pp. 1518–1527. https://doi.org/10.1016/j.cpc.2011.03.022

Binder K. (1997), "Applications of Monte Carlo methods to statistical physics", *Reports on Progress in Physics*, vol. 60, no. 5, pp. 487–559. https://doi.org/10.1088/0034-4885/60/5/001

Boneh D. and Lipton R.J. (1996), "Algorithms for black-box fields and their application to cryptography", *Lecture Notes in Computer Science*, vol. 1109, pp. 283–297. https://doi.org/10.1007/3-540-68697-5_22

Breiman L. (2001), "Random forests", *Machine Learning*, vol. 45, no. 1, pp. 5–32. https://doi.org/10.1023/A:1010933404324

Demchik V. (2011), "Pseudo-random number generators for Monte Carlo simulations on ATI graphics processing units", *Computer Physics Communications*, vol. 182, no. 3, pp. 692–705. https://doi.org/10.1016/j.cpc.2010.12.008

Dzhioeva I.K. and Tehov A.V. (2017), "Initial terms of development of enterprise are in Republic of South Ossetia", *Journal of Economy and entrepreneurship*, vol. 11, no. 9-2, pp. 434–438. (In Russian).

Djioeva I.K., Kochieva J.G., Techov A.V. and Dzhioeva A.K. (2018), “Strategy of restoration and increase of efficiency of the agro-food complex of the Republic of South Ossetia”, *Journal of Economy and entrepreneurship*, vol. 12, no. 2, pp. 335–342. (In Russian).

Djioeva I.K., Techov A.V. and Shelkunova T.G. (2019), “Key trends in the social economic transformation of modern society”, *Journal of Economy and entrepreneurship*, vol. 13, no. 8, pp. 293–295. (In Russian).

Fill J.A. (1998), “An interruptible algorithm for perfect sampling via Markov chains”, *The Annals of Applied Probability*, vol. 8, no. 1, pp. 131–162. https://doi.org/10.1145/258533.258664

Foulkes W.M.C., Mitas L., Needs R.J. and Rajagopal G. (2001), “Quantum Monte Carlo simulations of solids”, *Reviews of Modern Physics*, vol. 73, no. 1, pp. 33–83. https://doi.org/10.1103/REVMODPHYS.73.33

Frolova E.E., Polyakova T.A., Dudin M.N., Rusakova E.P. and Kucherenko P.A. (2018), “Information security of Russia in the digital economy: the economic and legal aspects”, *Journal of Advanced Research in Law and Economics*, vol. 9, no. 1, pp. 89–95. https://doi.org/10.14505/jarle.v9.1(31).12

Fürst M., Weier H., Nauerth S., Marangon D.G., Weinfurter H. and Kurtsiefer C. (2010), “High speed optical quantum random number generation”, *Optics Express*, vol. 18, no. 12, pp. 13029–13037. https://doi.org/10.1364/OE.18.013029

Gisin N., Ribordy G., Tittel W. and Zbinden H. (2002), “Quantum cryptography”, *Reviews of Modern Physics*, vol. 74, no. 1, pp. 145–195. https://doi.org/10.1103/REVMODPHYS.74.145

Hartley H.O. and Fitch E.R. (1951), “A chart for the incomplete beta-function and the cumulative binomial distribution”, *Biometrika*, vol. 38, no. 3-4, pp. 423–426. https://doi.org/10.2307/2332588

Hastings W.K. (1970), “Monte Carlo sampling methods using markov chains and their applications”, *Biometrika*, vol. 57, no. 1, pp. 97–109. https://doi.org/10.1093/biomet/57.1.97

Iskhakov T.Sh., Lopaeva E.D., Penin A.N., Rytikov G.O. and Chekhova M.V. (2008), “Two methods for detecting nonclassical correlations in parametric scattering of light”, *Journal of Experimental and Theoretical Physics Letters (JETP Letters)*, vol. 88, no. 10, pp. 660–664. https://doi.org/10.1134/S0021364008220050

Jennewein T., Achleitner U., Weihs G., Weinfurter H. and Zeilinger A. (1999), “A fast and compact quantum random number generator”, *Review of Scientific Instruments*, vol. 71, no. 4. pp. 1675–1680. https://doi.org/10.1063/1.1150518

Kamolov S.G. (2017), “Digital public governance: trends and risks”, *Journal of Constitutional History*, vol. 33, no. 1, pp.185–194.

Kim H.K. and Lebedev V. (2004), “On optimal superimposed codes”, *Journal of Combinatorial Design*, vol. 12, no. 2, pp. 79–91. https://doi.org/10.1002/jcd.10056

Liu J.-M., Chen H.-F. and Tang S. (2002), “Synchronized chaotic optical communications at high bit rates”, *IEEE Journal of Quantum Electronics*, vol. 38, no. 9, pp. 1184–1196. https://doi.org/10.1109/JQE.2002.802045

Maaranen H., Mäkelä M.M. and Miettinen K. (2004), “Quasi-random initial population for genetic algorithms”, *Computers & Mathematics with Applications*, vol. 47, no. 12, pp. 1885–1895. https://doi.org/10.1016/j.camwa.2003.07.011

Manssen M., Hartmann A.K. and Weigel M. (2012), “Random number generators for massively parallel simulations on GPU”, *The European Physical Journal. Special Topics*, vol. 210, no. 1, pp. 53–71. https://doi.org/10.1140/epjst/e2012-01637-8

Morozova A.N., Panov A.D., Pruchkina A.A., Rytikov G.O. and Tscherbina O.A. (2014), “Parametric down conversion frequency-angle spectrum modeling”, *2014 International Conference on Computer Technologies in Physical and Engineering Applications (ICCTPEA 2014)*, Saint-Petersburg, June 30–July 4, ed. E.I. Veremey, IEEE Catalog number: CFP14BDA-POD, St.- Petersburg, Russia, pp. 122–123. https://doi.org/10.1109/ICCTPEA.2014.6893314

Myasnikov A. and Roman’Kov V. (2015), “A linear decomposition attack”, *Groups, Complexity, Cryptology*, vol. 7, no. 1, pp. 81–94. https://doi.org/10.1515/gcc-2015-0007

Noh J.D. and Rieger H. (2004), “Random walks on complex networks”, Physical Review Letters, vol. 92, no. 11, ant. 118701. https://doi.org/10.1103/PhysRevLett.92.118701

Nyberg K. (1994), “Differentially uniform mappings for cryptography”, *Lecture Notes in Computer Science*, vol. 765, pp. 55–64. https://doi.org/10.10007/3-540-48285-7_6

Phillips C.L., Glotzer S.C. and Anderson J.A. (2011), “Pseudo-random number generation for brownian dynamics and dissipative particle dynamics simulations on GPU devices”, *Journal of Computational Physics*, vol. 230, no. 19, pp.7191–7201. https://doi.org/10.1016/j.jcp.2011.05.021

Rytikov GO. (2007), “Technique of approximate solution of a class of quantum optics problems”, *Vestnik MGUP imeni Ivana Fedorova*, no. 3, pp. 74–82. (In Russian).

Sobol I.M. (1998), “On quasi-Monte Carlo integrations”, *Mathematics and Computers in Simulation*, vol. 47, no. 2, pp. 103–112. https://doi.org/10.1016/S0378-4754(98)00096-2

Sobol I.M. and Levitan Yu.L (1999), “A pseudo-random number generator for personal computers”, *Computers & Mathematics with Applications*, vol. 37, no. 4-5, pp. 33–40. https://doi.org/10.1016/S0898-1221(99)00057-7

Soshnikov A. (2000), “Determinantal random point fields”, *Russian Mathematical Surveys*, vol. 55, no. 5, pp. 923–975. https://doi.org/10.1070/RM2000v055n05ABEH000321

Srinivasan A., Mascagni M. and Ceperley D. (2003), “Testing parallel random number generators”, *Parallel Computing*, vol. 29, no. 1, pp. 69–94. https://doi.org/10.1016/S0167-8191(02)00163-1

Steane A.M. (1998), “Quantum computing”, *Reports on Progress in Physics*, vol. 61, no. 2, pp. 117–173. https://dx.doi.org/10.1088/0034-4885/61/2/002

Tarone R.E. (1979), “Testing the goodness of fit of the binomial distribution”, *Biometrika*, vol. 66, no. 3, pp. 585–590. https://doi.org/10.1093/BIOMET/66.3.585

Vadhan S.P. (2011), “Pseudorandomness”, *Foundations and Trends in Theoretical Computer Science*, vol. 7, no. 1-3, pp. 1–336. https://doi.org/10.1561/0400000010

Wood S.N., Pya N. and Säfken B. (2016), “Smoothing parameter and model selection for general smooth models”, *Journal of the American Statistical Association*, vol. 111, no. 516, pp. 1548–1563. https://doi.org/10.1080/01621459.2016.1180986

Yang T., Yang L.B. and Yang C.M. (1998), “Cryptanalyzing chaotic secure communications using return maps”, *Physics Letters A*, vol. 245, no. 6, pp. 495–510. https://doi.org/10.1016/S0375-9601(98)00425-3

Yu W., Liang F., He X., Hatcher W.G., Lu C., Lin J. and Yang X. (2017), “A survey on the edge computing for the internet of things”, *IEEE Access*, vol. 6, pp. 6900–6919. https://doi.org/10.1109/ACCESS.2017.2778504