УДК 519.676, 519.24
MSC 65C10

Математическая модель квантового генератора случайных чисел на основе флуктуации вакуума

А. А. Гайдаш[1], *Р. К. Гончаров*[1], *А. В. Козубов*[1], *П. В. Яковлев*[2]

[1] Университет ИТМО,
Российская Федерация, 197101, Санкт-Петербург, Кронверкский пр., 49
[2] Санкт-Петербургский государственный университет,
Российская Федерация, 199034, Санкт-Петербург, Университетская наб., 7–9

Для цитирования: *Гайдаш А. А., Гончаров Р. К., Козубов А. В., Яковлев П. В.* Математическая модель квантового генератора случайных чисел на основе флуктуации вакуума // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2024. Т. 20. Вып. 2. С. 136–153. https://doi.org/10.21638/spbu10.2024.202

Рассматривается математическая модель широко распространенного физического квантового генератора случайных чисел на основе флуктуации вакуума. Приводится математическое обоснование «случайности» генерируемой последовательности в предположении об истинности основных постулатов квантовой теории и справедливости пуассоновского распределения вероятности для потока фотонов. Представлены результаты экспериментов и получены численные оценки минимальной энтропии.

Ключевые слова: квантовый генератор случайных чисел, оценка минимальной энтропии, флуктуация вакуума.

1. Описание оптической схемы. Случайные числа служат важным ресурсом в науке, технике и многих аспектах повседневной жизни. В частности, они есть неотъемлемая составляющая различных подходов к моделированию, построению криптографических систем и компьютерных сетей. В 50-х годах прошлого века развитие получил метод Монте-Карло (метод статистических испытаний), основой применения которого является одномерная равномерно распределенная на отрезке [0,1] случайная величина (см. [1]). Активно продолжает развиваться теория задачи поиска [2]. Во всех этих задачах высокая скорость выработки случайных битовых последовательностей и их степень случайности являются краеугольными факторами. К устройствам, создающим подобные последовательности, относятся и генераторы случайных чисел (ГСЧ).

В настоящее время все ГСЧ можно разделить на две группы: детерминированные, или псевдослучайные, и физические. Несмотря на высокую скорость генерации случайной последовательности, детерминированные ГСЧ имеют один ключевой недостаток — наличие цикла. Существует точка, после которой последовательность начинает повторяться. Физические ГСЧ основаны на сборе непредсказуемых данных в различных физических системах. Например, это может быть движение мышью компьютера или появление запроса в сети, тепловой шум процессора, атмосферный шум и т. д. Процесс сбора непредсказуемых данных обычно называют сбором энтропии. Рассматриваемый в этой работе ГСЧ относится к классу физических, а точнее, к его подклассу квантовых генераторов случайных чисел (КГСЧ). Подробный обзор КГСЧ содержится в [3]. Базовый принцип в построении оптической схемы устройства был

ранее представлен в работах [3–8]. Основным элементом подобных устройств является гомодинный детектор, детальный анализ которого можно найти в [9].

В данной работе приводится обоснование возможности создания КГСЧ, основанного на когерентном излучении одномодового лазера и флуктуации вакуума. Помимо этого, проводятся численное моделирование по расчету энтропии получаемой битовой последовательности, а также сравнение результатов моделирования с экспериментом.

2. Описание принципиальной схемы рассматриваемой модели КГСЧ. В общей структуре ГСЧ можно выделить два основных блока (рис. 1).

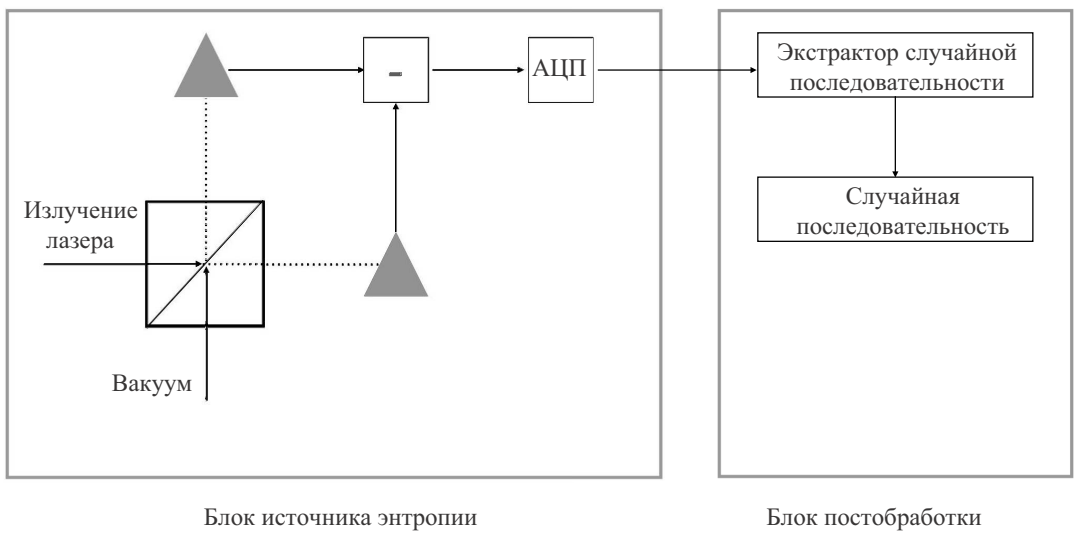

Рис. 1. КГСЧ на основе гомодинного детектора

Блок источника энтропии состоит из физической системы, характеризуемой некоторой «случайной» физической величиной, и измерительного оборудования, ее регистрирующего. Накопленные аналоговые измерения величин преобразовываются в битовые строки с помощью аналого-цифровых преобразователей (АЦП).

Основу гомодинного детектора [9, 10] составляет светоделитель. На два входа симметричного светоделителя с отношением 50:50 (рис. 2) подаются световые потоки с интенсивностями α и β. Следуя законам классической оптики, в случае, когда эти потоки на входе имеют по одной моде, амплитуды мод на выходе светоделителя будут равны $\dfrac{1}{\sqrt{2}}(\alpha+\beta)$, $\dfrac{1}{\sqrt{2}}(\alpha-\beta)$.

Переходя к квантовой трактовке, заменим интенсивности на квантовые состояния $|\alpha\rangle$ и $|\beta\rangle$. Если эти состояния когерентны и независимы, то на выходе светоделителя будем иметь состояния $\left|\dfrac{\alpha+\beta}{\sqrt{2}}\right\rangle$ и $\left|\dfrac{\alpha-\beta}{\sqrt{2}}\right\rangle$ соответственно. Измерение разности интенсивности поля на выходе светоделителя дает возможность оценить статистику фотоотсчетов (см. [9, с. 402]).

В общем случае, когда $|\alpha\rangle$ — когерентное состояние, а $|\beta\rangle$ имеет волновую функцию общего вида, статистика фотоотсчетов вычисляется аналитически. Если же оба потока когерентны и независимы, то вид распределения вероятности фотоотсчетов существенно упрощается. В рассматриваемом КГСЧ один вход светоделителя закрыт,

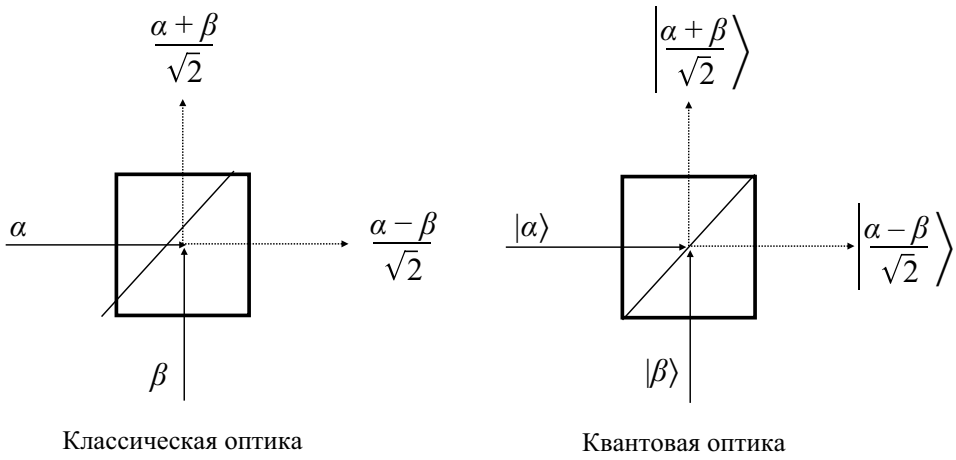

Рис. 2. Симметричный светоделитель

$|\hat{\beta}\rangle = |0\rangle$. В этом случае говорят (см. [3–6]), что измеряется состояние вакуума, который в квантовой трактовке является частным случаем когерентного состояния. Точнее говоря, когерентное состояние можно трактовать как смещенное состояние вакуума (см. [9, с. 336]). Отсюда происходит название «Генератор случайных чисел, основанный на флуктуации вакуума».

Блок постобработки получает на входе необработанную последовательность бит и формирует из них более короткую последовательность, свободную от корреляций. Данная операция называется экстракцией случайных бит и является важной составляющей КГСЧ. Экстракция случайных бит производится так называемой **хеш-функцией**, которая преобразует необработанную последовательность бит в последовательность бит с сохранением части или всей случайности входной последовательности и имеющей распределение, максимально близкое к равномерному. Компромисс выбора конкретной хеш-функции состоит в определении баланса между быстродействием и сохранением «случайности» (см. [11–14]).

3. Основные термины, определения и утверждения. Все дальнейшие обоснования энтропийности источника и «случайности» генерируемой последовательности чисел основываются на следующих предположениях.

1. Предполагаются верными постулаты квантовой теории света, в частности тот факт, что когерентное излучение одномодового лазерного источника представляет собой поток фотонов, являющийся однородным пуассоновским процессом, который описывается плотностью распределения

$$p_k(t) = \frac{(\nu t)^k}{k!} e^{-\nu t}$$

с интенсивностью $\nu[c^{-1}]$, или, в других обозначениях, $p_k(\lambda) = \frac{\lambda^k}{k!} e^{-\lambda}$, где $\lambda = \nu t$. Однородность пуассоновского потока означает, что его интенсивность ν не зависит от времени.

2. Все процессы стационарные. Считаем, что изменением интенсивности излучения лазера в пределах достаточно большого количества временных окон генерации случайных чисел, как и изменением параметров классических шумов, можно пренебречь.

3. Все процессы являются эргодическими. Стационарный случайный процесс называется эргодическим, если значение среднего и ковариационная функция, вычисленные по ансамблю выборочных функций, совпадают со средним и ковариационной функцией, определенными путем усреднения по времени в пределах отдельных выборочных функций, входящих в ансамбль.

4. Классический аппаратный (побочный) шум есть аддитивный независимый гауссовый процесс с нулевым средним $\mu_e = 0$ и дисперсией σ_e^2.

Рассмотрим процесс измерения флуктуации вакуума с точки зрения математической статистики и свойств пуассоновских процессов (потоков).

Определение 1 (Независимое смещение). Пусть $\{x_i(t)\}$, $i = 0, 1, \ldots,$ — случайная последовательность частиц на прямой, образующих при $t = 0$ стационарный пуассоновский поток. Координата каждой частицы $x_i(t)$ меняется случайным образом во времени t. Причем значения смещения за интервал времени от 0 до t, равные $x_i(t) - x_i(0)$, предполагаются независимыми и одинаково распределенными случайными величинами. Тогда такой процесс изменения координат называется независимым смещением.

Определение 2 (Операция разреживания). Пусть последовательность $\{x_i\}$, $i = 0, 1, \ldots,$ образует стационарный пуассоновский поток. Определим операцию разреживания следующим образом: каждая точка последовательности исключается из исходной последовательности с вероятностью γ, причем независимо от остальных, и делается одна и только одна попытка исключить каждую точку.

Утверждение 1. *Если в начальный момент времени $t = 0$ последовательность $\{x_i(0)\}$, $i = 0, 1, \ldots,$ образует стационарный пуассоновский процесс с интенсивностью ν, то при независимом смещении последовательность $\{x_i(t)\}, i = 0, 1, \ldots,$ в момент времени t также образует стационарный пуассоновский процесс с интенсивностью ν.*

Доказательство см. в [15].

Ввиду важности для обоснования энтропийности источника следующих утверждений, приведем их доказательства.

Утверждение 2. *Если к пуассоновскому процессу с интенсивностью ν применяется операция разреживания с вероятностью исключения γ, то оставшийся поток является пуассоновским с интенсивностью $(1 - \gamma)\nu$.*

Доказательство. Справедливость утверждения 2 следует из выполнения определяющих свойств пуассоновского процесса:

1) ординарность: вероятность наступления более одного события на любом малом интервале времени Δt имеет более высокий порядок малости, чем Δt;

2) стационарность;

3) отсутствие последствий: имеет независимые приращения на неперекрывающихся промежутках времени.

Условие ординарности означает, что

$$P(x_i(t + \Delta t) - x_i(t) = 1) = P(x_i(\Delta t) = 1) = \nu \Delta t + o(\Delta t),$$

$$P(x_i(t + \Delta t) - x_i(t) > 1) = P(x_i(\Delta t) > 1) = o(\Delta t).$$

При операции разреживания ординарность сохраняется, так как количество точек может только уменьшиться.

Стационарность сохраняется, поскольку операция разреживания производится одинаково при любом значении x_i.

И, наконец, в силу того, что исключение точек происходит всегда независимо от предыдущих исключений, сохраняется свойство отсутствия последствий.

Известно (см. [15]), что случайный процесс, удовлетворяющий перечисленным трем свойствам, является пуассоновским, а удаление точек с вероятностью γ уменьшает интенсивность потока на коэффициент $(1-\gamma)$. □

Следствие. *В случае, если к пуассоновскому процессу с интенсивностью ν применить операцию разреживания с вероятностью исключения $\gamma = \frac{1}{2}$, то разреженный процесс и процесс, составленный из удаляемых точек, будут пуассоновскими с интенсивностью $\frac{1}{2}\nu$.*

Утверждение 3. *Разность двух пуассоновских процессов $u_i = x_i - y_i$ с интенсивностями α и μ соответственно имеет распределение*

$$P_u(k) = e^{-(\alpha+\mu)t}(\tfrac{\alpha}{\mu})^{\frac{k}{2}} I_k(2\sqrt{\alpha\mu}t),$$

где $I_k(z)$ — модифицированная функция Бесселя первого рода целого порядка.

Доказательство. Найдем распределение случайной величины $u = x - y$, в котором величины x и y имеют пуассоновское распределение вероятности

$$P_x(n) = \frac{(\alpha t)^n}{n!}e^{-\mu t}, \quad P_y(n) = \frac{(\mu t)^n}{n!}e^{-\mu t}.$$

Запишем распределение вероятности для величины $u = x - y$:

$$P_u(k) = \mathsf{P}(u = k) = \sum_{l=0}^{\infty} \mathsf{P}(x = k + l)\,\mathsf{P}(y = l) =$$

$$= e^{-(\alpha+\mu)t} \sum_{l=0}^{\infty} \frac{(\alpha t)^{k+l}(\mu t)^l}{(k+l)!\; l!} = e^{-(\alpha+\mu)t}(\alpha t)^k \sum_{l=0}^{\infty} \frac{(\sqrt{\alpha\mu}t)^{2l}}{(k+l)!\; l!}.$$

Воспользуемся разложением в ряд модифицированной функции Бесселя первого рода целого порядка (см. [16])

$$I_k(z) = (\tfrac{z}{2})^k \sum_{l=0}^{\infty} \frac{(\frac{z}{2})^{2l}}{(k+l)!\; l!}$$

и положим, что $z = 2\sqrt{\alpha\mu}t$. Тогда искомое распределение приобретает требуемый вид

$$P_u(k) = e^{-(\alpha+\mu)t}(\tfrac{\alpha}{\mu})^{\frac{k}{2}} I_k(2\sqrt{\alpha\mu}t). \tag{1}$$

□

Следствие. *В случае, когда вычитаются два пуассоновских процесса с одинаковыми интенсивностями $\alpha = \mu$, результирующий процесс имеет распределение*

$$\mathsf{P}_u(k) = e^{-2\alpha t} I_k(2\alpha t).$$

В дальнейшем функцию вероятности пуассоновского процесса с интенсивностью α будем записывать следующим образом:

$$p_k(\lambda) = \frac{\lambda^k}{k!}e^{-\lambda},$$

здесь $\lambda = \alpha t$.

Утверждение 4. *Разность двух пуассоновских процессов $u_i = x_i - y_i$ с одинаковым средним λ при большой интенсивности аппроксимируется нормальным (гауссовым) распределением со средним $\mu = 0$ и дисперсией $\sigma^2 = \lambda$:*

$$p_k(\lambda) \approx \frac{1}{\sqrt{2\pi\lambda}} e^{-\frac{k^2}{2\lambda}}.$$

Д о к а з а т е л ь с т в о. Оно следует из аппроксимации функции Бесселя при фиксированном значении k для больших величин λ (см. [16, с. 199]):

$$I_k(\lambda) = \frac{e^\lambda}{\sqrt{2\pi\lambda}} \left[1 + \sum_{n=1}^{\infty} (-1)^n \frac{(\mu-1)(\mu-3^2)\cdots(\mu-(2n-1)^2)}{n!(8\lambda)^n} \right],$$

где $\mu = 4k^2$. При больших значениях λ получаем, что

$$I_k(\lambda) \approx \frac{e^\lambda}{\sqrt{2\pi\lambda}} \left[1 + \sum_{n=1}^{\infty} (-1)^n \frac{(k^2)^n}{n!(2\lambda)^n} \right] = \frac{e^\lambda}{\sqrt{2\pi\lambda}} e^{-\frac{k^2}{2\lambda}}.$$

Окончательно имеем, что

$$p_k(\lambda) \approx \frac{1}{\sqrt{2\pi\lambda}} e^{-\frac{k^2}{2\lambda}}.$$

□

Частный случай разности двух пуассоновских процессов с равными средними значениями был получен в 1937 г. Дж. Ирвином (см. [17]), общий случай в 1946 г. рассмотрел Дж. Г. Скеллам (см. [18]). Доказательство утверждений 2 и 3 приведено в соответствии с [15].

Среднее значение λ количества фотонов в потоке излучения лазера, рассматриваемого в качестве конкретного источника, рассчитывается по формуле

$$\lambda = \frac{PT}{\hbar\omega} \approx 3.9 \cdot 10^8,$$

в которой $\hbar$ — редуцированная постоянная Планка, $T = 10^{-9}$ — время усреднения, определяемое частотой дискретизации 1 ГГц, $\omega \approx 2\pi 1.93414 \cdot 10^{-14}$ — круговая частота лазера с длиной волны 1550 нм, $P = 5 \cdot 10^{-3}$ В — мощность лазера. Данное значение λ позволяет воспользоваться асимптотическим поведением измеряемого случайного процесса.

Приведенное выше обоснование формулы распределения случайного процесса, описывающего измерение величины на выходе гомодинного детектора (утверждения 2, 3), аналогично обоснованиям, использующим обозначения и терминологию, принятые в квантовой оптике [9, 19]. Во всех случаях основой производимых расчетов являются два основополагающих факта:

• количество фотонов в потоке описывается распределением Пуассона;

• светоделитель гомодинного детектора разделяет поток фотонов в равной пропорции 50:50 в соответствии с приведенным определением 2.

В обширной литературе, посвященной КГСЧ, основанных на флуктуации вакуума, вопрос о виде распределения случайной величины, измеряемой на выходе гомодинного детектора, часто опускается. Предполагают, что сигнал на выходе гомодинного детектора описывается нормальным (гауссовым) законом распределения (см. [4–8]).

Основываясь на сделанных предположениях и приведенных выше утверждениях, можно сделать вывод, что когерентное лазерное излучение генерирует случайный стационарный поток фотонов, подчиняющийся распределению Пуассона со средним значением λ за время T, равное интервалу детектирования (дискретизации).

Далее пуассоновский поток фотонов, проходя через гомодинный детектор, разделяется при помощи симметричного светоделителя на два пуассоновских потока с одинаковым средним значением $\frac{1}{2}\lambda$, после чего происходит их вычитание. В результате получается случайный стационарный поток фотонов, асимптотически описываемый гауссовым законом распределения с нулевым средним и дисперсией $\sigma^2 = \lambda$.

4. Оценка минимальной энтропии. Для того чтобы воспользоваться результатом леммы об остаточном хеше и построить хеш-функцию, извлекающую последовательность случайных бит, близких к равномерному распределению, необходимо оценить значение минимальной энтропии условного распределения дискретного сигнала при условии наличия шума.

Для идеального случая, когда наблюдаем только результат измерения состояния вакуума без посторонних шумов, можно получить верхнюю границу минимальной энтропии для рассматриваемого источника излучения

$$H_{\min}(X) = -\log_2(\max_k p_k(\lambda)) = -\log_2\left(\frac{1}{\sqrt{2\pi\lambda}}\right) \approx \log_2(\sqrt{2\pi 3.9 \cdot 10^8}) \approx 15.59 \text{ бит}. \quad (2)$$

Для оценки условной минимальной энтропии при наличии шума воспользуемся сделанными в п. 3 предположениями о процессах. Считаем, что сигнал x, подаваемый на вход АЦП, является суммой двух независимых стационарных гауссовых процессов с нулевым средним: полезного квантового сигнала x_q (флуктуация вакуума) и шума x_e, $x = x_q + x_e$ со средними $\mu_q = \mu_e = 0$ и дисперсиями $\sigma_q^2, \sigma_e^2, \sigma_x^2 = \sigma_q^2 + \sigma_e^2$. Тогда, учитывая последнее предположение, плотность условного распределения измеряемого сигнала x при наличии шума x_e равна (см. [20])

$$p(x|x_e) = \frac{1}{\sqrt{2\pi(\sigma_x^2 - \sigma_e^2)}} e^{-\frac{(x-x_e)^2}{2(\sigma_x^2-\sigma_e^2)}} = \frac{1}{\sqrt{2\pi}\sigma_q} e^{-\frac{(x-x_e)^2}{2\sigma_q^2}},$$

а для условной минимальной энтропии измеряемого сигнала при наличии шума запишем, что

$$H_{\min}(X|E) = -\log_2\left(\max_{x_e \in \{x_e \in E | p(x_e) > 0\}} \max_{x_i \in X} \mathsf{P}(x_i|x_e)\right), \quad (3)$$

где x_i и e_i — дискретные значения измеряемого сигнала и шума соответственно.

Рассмотрим идеальное АЦП с n двоичными разрядами, динамическим диапазоном $[-R, R]$, интервалом квантования $\delta = \frac{R}{2^{n-1}}$ и нулем в середине центрального интервала. Обозначим границы интервалов квантования через $\{m_1, m_2, \ldots, m_{2^n+1}\}, m_1 = -R, m_{2^n+1} = R$. Введем два дополнительных узла квантования $m_0 = -\infty$ и $m_{2^n+2} = +\infty$. Тогда, производя интегрирование в выражении для условной минимальной энтропии (3), получаем, что

$$H_{\min}(X|E) = -\log_2\left(\max_{x_e \in \{x_e \in E | p(x_e) > 0\}} \max_{i \in 0:2^n+1} \frac{1}{\sqrt{2\pi}\sigma_q} \int_{m_i}^{m_{i+1}} e^{-\frac{(x-x_e)^2}{2\sigma_q^2}} dx\right).$$

Рассмотрим выражение $\max\limits_{i\in 1:2^n} \frac{1}{\sqrt{2\pi}\sigma_q} \int\limits_{m_i}^{m_{i+1}} e^{-\frac{(x-x_e)^2}{2\sigma_q^2}} dx$ в пределах динамического диапазона $[-R, R]$. Находим, что

$$\max_{i\in 1:2^n} \frac{1}{\sqrt{2\pi}\sigma_q} \int\limits_{m_i}^{m_{i+1}} e^{-\frac{(x-x_e)^2}{2\sigma_q^2}} dx = \max_{i\in 1:2^n} \frac{1}{\sqrt{\pi}} \int\limits_{u_i}^{u_i+\tilde{\delta}} e^{-u^2} du = \frac{1}{2}(\mathrm{erf}(\tfrac{\tilde{\delta}}{2}) - \mathrm{erf}(-\tfrac{\tilde{\delta}}{2})) =$$

$$= \mathrm{erf}(\tfrac{\tilde{\delta}}{2}) = \mathrm{erf}(\tfrac{\delta}{2\sqrt{2}\sigma_q}),$$

где $\tilde{\delta} = \frac{\delta}{\sqrt{2}\sigma_q}$; $u = \frac{x-x_e}{\sqrt{2}\sigma_q}$; $\mathrm{erf}(x) = \frac{2}{\sqrt{\pi}} \int\limits_0^x e^{-u^2} du$ — функция ошибок. Такое значение максимума обусловлено тем, что функция ошибок имеет максимальное приращение вблизи нуля. В рассматриваемом случае это интервал интегрирования с центром в нуле.

Добавляя два бесконечных интервала $[-\infty, -R]$ и $[R, \infty]$, получим, что

$$H_{\min}(X|E) = -\log_2 \left(\max_{x_e\in\{x_e\in E|p(x_e)>0\}} \max \begin{cases} \frac{1}{2}\left(1 - \mathrm{erf}(\frac{x_e+R}{\sqrt{2}\sigma_q})\right), \\ \mathrm{erf}(\frac{\delta}{2\sqrt{2}\sigma_q}), \\ \frac{1}{2}\left(\mathrm{erf}(\frac{x_e-R}{\sqrt{2}\sigma_q}) + 1\right) \end{cases} \right).$$

Легко заметить, что выражение под знаком логарифма стремится к единице, когда $x_e \to -\infty$ или $x_e \to +\infty$. Поэтому для практической оценки вынуждены ограничиться рассмотрением случая, когда значение постороннего шума ограничено в диапазоне $[e_{\min}, e_{\max}]$. Например, если возьмем диапазон $e_{\min} = -5\sigma_e$, $e_{\max} = 5\sigma_e$, то значение шума попадет в него в 99.9999 % случаев.

Тогда, если $e_{\min} = e_{\max}$, оценка минимальной энтропии приобретает вид

$$H_{\min}(X|E) = -\log_2 \left(\max \left\{ \frac{1}{2}\left(1 - \mathrm{erf}(\tfrac{e_{\min}+R}{\sqrt{2}\sigma_q})\right), \mathrm{erf}(\tfrac{\delta}{2\sqrt{2}\sigma_q}) \right\} \right). \tag{4}$$

Вопрос выбора оптимальных параметров дискретизации (количество бит, динамический диапазон) рассмотрен в [21].

4.1. Учет нелинейных искажений АЦП. Основными искажениями АЦП, которые могут повлиять на энтропию измеряемого цифрового сигнала, являются дифференциальная нелинейность (DNL — Differential Nonlinearity) и ошибка смещения (offset error). Дифференциальная нелинейность измеряется в долях от величины интервала квантования, или, другими словами, в процентах от младшего разряда (LSB — Least Significant Bit), ошибка смещения — в процентах от динамического диапазона (FSR — Full Scale Range). Обозначим эти ошибки соответственно через $\Delta_{\mathrm{dnl}}, \Delta_{\mathrm{off}s}$. Дифференциальная нелинейность может увеличить длину интервала интегрирования с δ до $\hat{\delta} = \delta(1 + \Delta_{\mathrm{dnl}})$. Тогда оценка минимальной энтропии изменится следующим образом:

$$H_{\min}(X|E) = -\log_2 \left(\max \left\{ \frac{1}{2}\left(1 - \mathrm{erf}(\tfrac{e_{\min}+\Delta_{\mathrm{off}s}+R}{\sqrt{2}\sigma_q})\right), \mathrm{erf}(\tfrac{\hat{\delta}}{2\sqrt{2}\sigma_q}) \right\} \right).$$

Интегральная нелинейность АЦП (INL — Integral Nonlinearity) по сути представляет собой сумму дифференциальных нелинейностей, поэтому не оказывает влияния на величину минимальной энтропии, так как определяющим является максимальное значение вероятности на каком-либо из интервалов дискретизации. Ошибкой смещения также можно пренебречь в случае достаточной ширины динамического диапазона АЦП. Например, при дифференциальной нелинейности 1.5 LSB оценка минимальной энтропии уменьшается на 1.32 бит равномерно по разрядности АЦП.

4.2. Параметры расчета оценки минимальной энтропии. Поскольку нет возможности оценивать шумовые параметры и искажения, производимые каждым конкретным экземпляром устройства, то единственным корректным источником оценки минимальной энтропии являются паспортные характеристики используемых в устройстве модулей и их подтверждение в процессе испытаний:

- отношение сигнал/шум $\mathrm{SNR} = 20\log_{10}\dfrac{\sigma_q}{\sigma_e}$, которое может быть оценено по паспортным данным лазера, гомодинного детектора и других компонентов КГСЧ;
- динамический диапазон АЦП (R);
- разрядность АЦП и δ — величина младшего значащего разряда (LSB);
- дифференциальная нелинейность и ошибка смещения $\Delta_{\mathrm{dnl}}, \Delta_{\mathrm{offs}}$.

Влияние снижения мощности лазера на значение минимальной энтропии оценивается, исходя из формулы (2); так, при уменьшении мощности лазера с 50 до 10 мВ верхняя оценка минимальной энтропии понижается всего на 1 бит — с 15.6 до 14.6 бит.

Нарушение балансировки симметричного светоделителя приводит к смещению среднего значения итогового распределения. Пусть пуассоновский поток со средним значением λ делится в соотношении γ и $(1-\gamma)$, где $\gamma \in (0,1)$. Из формулы (1) и аппроксимации модифицированной функции Бесселя следует, что разность таких потоков будет иметь смещенное среднее $\tilde{\lambda} = \lambda\sqrt{\gamma(1-\gamma)}\ln\dfrac{\gamma}{1-\gamma}$. Если смещение балансировки светоделителя не выводит сигнал из динамического диапазона АЦП, то это не приведет к изменению минимальной энтропии. В противном случае существенное смещение должен выявить встроенный тест устройства.

4.3. Влияние ограниченности полосы пропускания гомодинного детектора. Используемый в рассматриваемой схеме гомодинный детектор является линейным устройством. Искажения, которым подвержен сигнал, проходящий через него, обусловлены:

- наличием независимого аддитивного гауссова шума, который учитывается при оценке минимальной энтропии в параметре сигнал/шум;
- ограниченностью полосы пропускания детектора, которая приводит к изменению спектральной плотности сигнала и соответственно его функции автокорреляции.

Воспользуемся свойствами гауссовых случайных процессов: 1) если A — инвариантный во времени линейный оператор, $x(t)$ — стационарный случайный гауссов процесс, то $A(x(t))$ также является стационарным гауссовым процессом; 2) гауссов стационарный случайный процесс с нулевым средним полностью определяется функцией спектральной плотности.

Рассмотрим стационарный случайный процесс $x(t)$ с нулевым средним.

Обозначим $S_{xx}(f) = \int\limits_{-\infty}^{\infty} R_{xx}(\tau)e^{-i2\pi f\tau}d\tau = 2\int\limits_{0}^{\infty} R_{xx}(\tau)\cos(2\pi f\tau)d\tau$ — спектральную плотность процесса $x(t)$, где $R_{xx}(\tau)$ — функция автокорреляции. Односто-

ронняя спектральная плотность равна $G_{xx} = \begin{cases} 2S_{xx}(f), & f \geqslant 0, \\ 0, & f < 0. \end{cases}$ Тогда $R_{xx}(\tau) = \int\limits_0^\infty G_{xx}(f)\cos(2\pi f\tau)df$, и дисперсия $\sigma_x^2 = R_{xx}(0) = \int\limits_0^\infty G_{xx}(f)df$.

Введем понятия **эффективной шумовой ширины спектра** и **эффективного шумового времени корреляции** (см. [22]). Эффективная шумовая ширина спектра, по определению, равна

$$B_x = \frac{\int\limits_0^\infty G_{xx}(f)df}{\max\limits_{f\in[0,\infty)} G_{xx}(f)} = \frac{R_{xx}(0)}{\max\limits_{f\in[0,\infty)} G_{xx}(f)},$$

а эффективное шумовое время корреляции определяется по формуле

$$T_x = \frac{\int\limits_{-\infty}^\infty |R_{xx}(\tau)|d\tau}{\max\limits_{\tau\in[0,\infty)} R_{xx}(\tau)} = \frac{2\int\limits_0^\infty |R_{xx}(\tau)|d\tau}{R_{xx}(0)}.$$

Нетрудно показать, что выполняется так называемое **соотношение неопределенности**

$$B_xT_x = \frac{2\int\limits_0^\infty |R_{xx}(\tau)|d\tau}{\max\limits_{f\in[0,\infty)} G_{xx}(f)} \geqslant \frac{1}{2}\,.$$

Для гауссова нормального шума с нулевым средним и дисперсией σ_x^2 данные величины равны

$$B_x = \frac{\sigma_x\sqrt{\pi}}{\sqrt{2}} \approx 1.25\sigma_x, \quad T_x = \frac{1}{\sigma_x\sqrt{2\pi}} \approx \frac{0.40}{\sigma_x},$$

$$B_xT_x = \frac{1}{2}\,.$$

Соотношение неопределенности говорит о том, что чем меньше эффективная шумовая ширина спектра, тем больше эффективное шумовое время корреляции.

Обозначим $H(f)$ — частотную характеристику гомодинного детектора, которая представляет собой фильтр нижних частот. Тогда односторонняя спектральная плотность выходного сигнала $y(t)$ будет равна $Gyy(f) = |H(f)|^2G_{xx}(f)$. Для стационарного гауссова процесса $y(t)$ дисперсия равна

$$\sigma_y^2 = \int\limits_0^\infty G_{yy}(f)df = R_{yy}(0) = \int\limits_0^\infty |H(f)|^2G_{xx}(f)df.$$

Поэтому, если полоса пропускания низкочастотного фильтра $H(f)$ намного шире эффективной шумовой ширины спектра сигнала $x(t)$, то влиянием данного фильтра на дисперсию сигнала можно пренебречь.

Для рассматриваемого в работе устройства ширина полосы пропускания гомодинного детектора равна 1.6 ГГц, в то время как дисперсия сигнала $\sigma_x^2 \approx 3.9\cdot10^8$. Таким образом, эффективная шумовая ширина спектра сигнала $B_x \approx 2.0\cdot10^4 \ll 1.6\cdot10^9$, и изменением дисперсии можно пренебречь.

Подтверждение того, что ограниченная полоса пропускания рассматриваемого устройства не оказывает влияния на дисперсию, можно получить, сравнив расчетную и фактическую величины дисперсии сигнала.

Кроме того, в обосновании энтропийности источника случайных чисел используется только дисперсия и нигде не применяется конкретный вид спектральной плотности сигнала и его автокорреляционной функции.

Ограниченность полосы пропускания уменьшает как дисперсию сигнала, так и дисперсию постороннего шума. Этим можно воспользоваться, чтобы увеличить отношение сигнал/шум. Если имеется априорная информация о спектре постороннего классического шума, то можно отфильтровать частоты с малым отношением сигнал/шум. Например, если энергия постороннего шума на нижних частотах $f \in [0, f_0]$ преобладает над уровнем энергии квантового шума на тех же частотах, то можно использовать полосовой фильтр, убирающий данные частоты, и увеличить отношение

$$\frac{\sigma_q^2}{\sigma_e^2} \leqslant \frac{\hat{\sigma}_q^2}{\hat{\sigma}_e^2} = \frac{\int\limits_{f_0}^{\infty} G_{xx}(f)df}{\int\limits_{f_0}^{\infty} G_{ee}(f)df},$$

где $G_{ee}(f)$ — односторонняя спектральная плотность шума.

Ограниченность полосы пропускания детектора можно учитывать разными эквивалентными способами. Например, в работе [7] влияние ограниченности полосы пропускания и появление временных автокорреляций рассматриваются в рамках понятия независимых одинаково распределенных величин (НОР) (identical and independent distribution, i.i.d.). Данное понятие применяется к случайным процессам с дискретным временем, поэтому появление автокорреляции оценивается через среднее число регистрируемых фотонов в дискретные моменты времени. Авторы статьи [7] отвергают гипотезу НОР, предполагают зависимость количества регистрируемых фотонов от предыдущих измерений (вследствие ограниченности полосы пропускания детектора) и вносят соответствующую поправку в расчет дисперсии.

В предлагаемой методике переходим к непрерывной модели измеряемого сигнала. Передаточные функции гомодинного детектора, как и других компонентов, входящих в устройство, изменяют спектральную плотность мощности сигнала и его автокорреляционную функцию. Поэтому отсчеты сигнала, получаемые на выходе АЦП, не могут рассматриваться как независимые одинаково распределенные величины, т. е. гипотеза НОР отвергается в момент перехода к непрерывному гауссову процессу. Тем не менее это не мешает получить корректную оценку минимальной энтропии, поскольку в ней не учитывается конкретный вид спектра и автокорреляционной функции сигнала, а используются только независимость и гауссовость сигнала и шума, а также значения их дисперсий.

5. Численное моделирование и результаты экспериментов. Для проведения экспериментальных расчетов и сравнения с результатами моделирования применялся тестовый сигнал, являющийся измерением флуктуации вакуума при помощи гомодинного детектора. Для измерения использовался одномодовый лазер с длиной волны 1550 нм, мощностью $P = 5 \cdot 10^{-3}$ В и АЦП с разрядностью 12 бит и частотой дискретизации 1 ГГц.

Гистограмма тестового сигнала приведена на рис. 3. Обозначим через $\hat{\sigma}$ оценку среднеквадратического отклонения распределения вероятности тестового сигнала. Динамический диапазон АЦП в данном эксперименте составил $R \approx 4.44 \cdot \hat{\sigma}$. Для моде-

лирования полезного квантового сигнала было использовано нормальное (гауссово) распределение с нулевым средним и дисперсией, равной дискретной оценке дисперсии тестового сигнала: $\sigma_q^2 = \hat{\sigma}^2$.

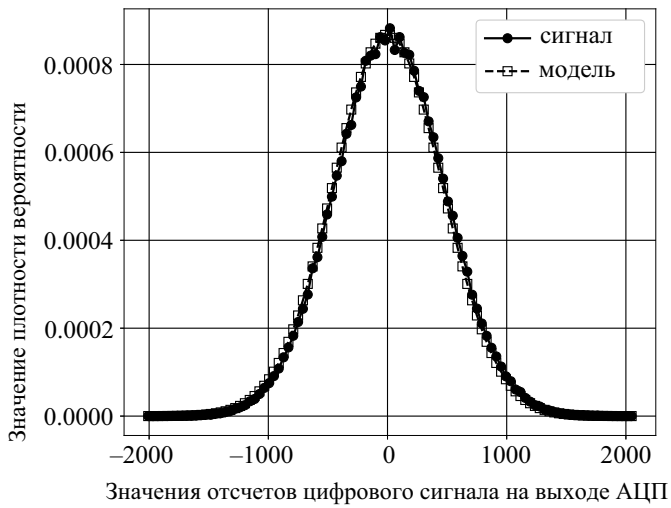

Рис. 3. Гистограмма тестового сигнала

Уровень постороннего шума, являющегося, по нашему предположению, независимым, стационарным гауссовым процессом, задается значением отношения сигнал/шум (SNR).

Рисунки 4, 5 иллюстрируют сравнение зависимости максимума дискретной плотности вероятности и дискретной оценки минимальной энтропии от разрядности АЦП для модельного и тестового сигналов. Можно заметить, что имеются небольшие расхождения для модельного и тестового сигналов для крайних значений разрядности АЦП, равных 3 и 10–11 бит. При малом количестве бит такое расхождение можно объяснить смещением при моделировании пороговых значений дискретизации (offset error), которое может не совпадать со смещением дискретизации тестового сигнала и имеет большой относительный вес при малой разрядности. Возможно, для значений разрядности 10–12 бит проявляется отклонение параметров сигналов, поскольку тестовый сигнал уже содержит посторонний шум.

В соответствии с формулой (4) при оценке минимальной энтропии учитывается вероятность попадания зашумленного сигнала за пределы динамического диапазона АЦП («хвостовая составляющая»). На рис. 6 приведена зависимость оценки минимальной энтропии от разрядности АЦП и отношения сигнал/шум. Пунктирной линией обозначена «хвостовая составляющая» минимальной энтропии, которая зависит от динамического диапазона АЦП. Видно, что при значении границы динамического диапазона $R \approx 4.44 \cdot \hat{\sigma}$ и максимальном уровне шума $e_{\min} = -5\sigma_e, e_{\max} = 5\sigma_e$, начиная от уровня сигнал/шум выше 10 дБ, определяющей является центральная часть области определения функции плотности распределения вероятности сигнала.

6. Экстракция равномерной случайной последовательности. Формирование (экстракция) равномерно распределенной последовательности бит из исходной случайной последовательности бит, имеющей произвольную функцию вероятности

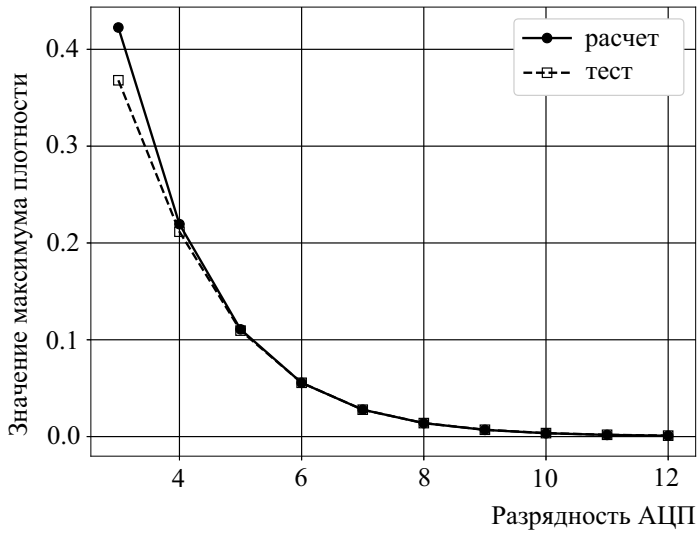

Рис. 4. Зависимость максимума дискретной плотности вероятности от разрядности АЦП

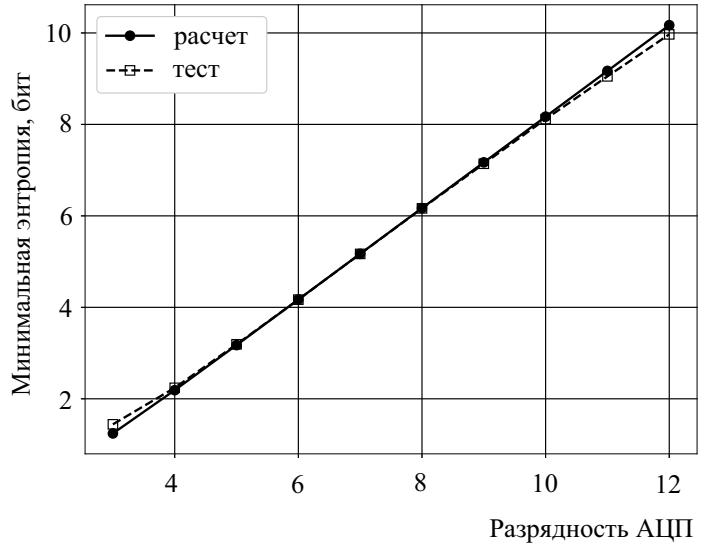

Рис. 5. Зависимость минимальной энтропии от разрядности АЦП

и заданный уровень минимальной энтропии, основано на лемме об остаточном хеше (см. [11] и с. 149).

Определение 3. Семейство функций $h \in H$, отображающих множество A в множество B, называется семейством универсальных хеш-функций, если для любых элементов $a_1, a_2 \in A, a_1 \neq a_2$ и $b_1, b_2 \in B$ вероятность совпадения образов обратно пропорциональна квадрату мощности множества B:

$$\mathsf{P}_{h \in H}\{h(a_1) = b_1 \wedge h(a_1) = b_1\} = \frac{1}{|B|^2}.$$

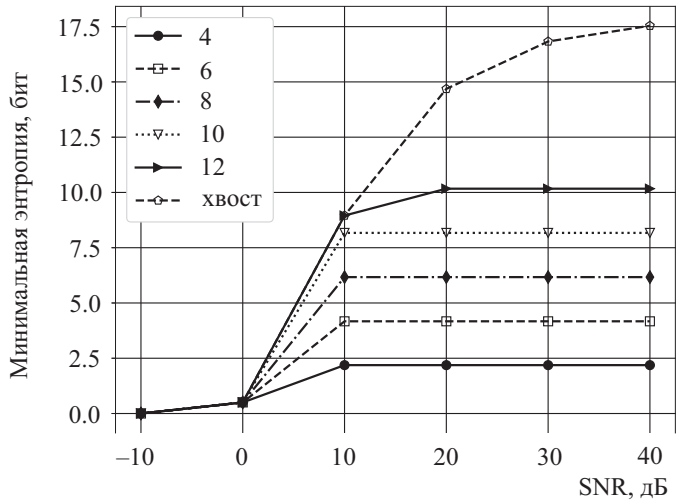

Рис. 6. Зависимость энтропии модельного сигнала от отношения SNR

Определенное на с. 147 семейство хеш-функций часто называют универсальным семейством хеш-функций второго рода (two-universal hash functions).

Определение 4. Экстрактором случайных бит называется функция, отображающая случайную последовательность бит, с, вообще говоря, неизвестным распределением вероятности, в другую, более короткую последовательность случайных бит, распределенных по закону, близкому к равномерному:

$$T : x = \{0,1\}^n \to y = \{0,1\}^m.$$

Определение 5. Экстрактором Теплица называется экстрактор, определенный при помощи матрицы Теплица, элементы которой состоят из нулей и единиц, выбранных случайным образом, а генерируемая строка бит получается умножением данной матрицы на вектор исходной последовательности по модулю 2:

$$T = T[1:l, 1:n],\ T[i,j] = T[i-1, j-1],$$
$$y[1:l] = (T[1:m, 1:n] \cdot x[1:n]) \mod 2.$$

Определение 6. Два вероятностных распределения X и Y, заданных в одной и той же области определения Z, называются ϵ-близкими, если

$$\max_{V \subseteq Z} \left\| \sum_{v \in V} (\mathsf{P}(X = v) - \mathsf{P}(Y = v)) \right\| \leqslant \epsilon.$$

Утверждение 5. *Семейство хеш-функций, состоящих из экстракторов Теплица со случайно выбранными элементами, является универсальным семейством хеш-функций второго рода.*

Доказательство утверждения см. в [13].

Лемма (Лемма об остаточном хеше). *Пусть X — случайная величина, $H_{\min}(X|E)$ — минимальная энтропия X при условии E. Пусть F — семейство универсальных хеш-функций второго рода из X в $\{0,1\}^l$. Тогда среднее распределение по $f \in F$ будет ϵ-близко к равномерному распределению, где*

$$\epsilon = \frac{1}{2}\sqrt{2^{l-H_{\min}(X|E)}}.$$

Доказательство леммы об остаточном хеше см. в [11].

В качестве следствия к лемме об остаточном хеше получаем, что из случайной последовательности $x \in X$ длиной n бит можно извлечь l случайных бит, ϵ-близких к равномерно распределенной последовательности при

$$l = \lfloor nH_{\min}(X|E) - \log_2 \frac{1}{\epsilon^2} + 2 \rfloor. \tag{5}$$

7. Заключение. Была рассмотрена математическая модель физического КГСЧ, основанного на когерентном излучении одномодового лазера. Физическим источником энтропии служит случайный поток фотонов лазерного излучения, подчиняющийся пуассоновскому распределению вероятностей. Использование для измерения гомодинного детектора, в котором исходное излучение является опорным сигналом, приводит к так называемому измерению флуктуации вакуума (нулевого квантового состояния), что дает широко распространенное название таких КГСЧ: «Квантовый генератор случайных чисел, основанный на флуктуации вакуума». Приведенные математические утверждения позволяют четко определить источник энтропии и сделать вывод о «случайности» генерируемой последовательности чисел в рамках сделанных предположений.

Результаты численных экспериментов показывают, что рассматриваемая математическая модель хорошо согласуется с экспериментом.

Для КГСЧ, включающем в качестве основных компонентов

- лазер с длиной волны 1550 нм и мощностью $5 \cdot 10^{-3}$ В,
- гомодинный детектор с симметричным светоделителем,
- АЦП 14 бит, частота дискретизации 1–1.25 ГГц,

можно получить последовательность случайных чисел с минимальной энтропией 10–12 бит в зависимости от уровня шума входящих в КГСЧ компонентов. При этом приведенная выше верхняя оценка минимальной энтропии составляет $H_{\min}(X) \approx 15.59$ бит.

Скорость генерации случайной последовательности для конкретного устройства можно получить, задав требуемое допустимое отклонение от равномерного распределения и расчетную оценку минимальной энтропии, с учетом шумовых параметров устройства.

Литература

1. *Ермаков С. М.* Метод Монте-Карло и смежные вопросы. М.: Наука, 1975. 472 с.

2. *Прокаев А. Н.* Принцип максимума энтропии в теории поиска // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2023. Т. 19. Вып. 1. С. 27–42. https://doi.org/10.21638/11701/spbu10.2023.103

3. *Herrero-Collantes M., Garcia-Escartin J. C.* Quantum random number generators // Rev. Mod. Phys. 2017. Vol. 89. N 2. Art. N 015004. https://doi.org/10.1103/RevModPhys.89.015004

4. *Gabriel C., Wittmann C., Sych D., Dong R., Mauerer W., Andersen U. L., Marquardt C., Leuchs G.* A generator for unique quantum random numbers based on vacuum states // Nature Photon. 2010. N 4. P. 711–715. https://doi.org/10.1038/nphoton.2010.197

5. *Shi Y., Chng B., Kurtsiefer C.* Random numbers from vacuum fluctuations // Applied Physics Letters. 2016. Vol. 109. N 4. Art. N 041101. P. 1–5 https://doi.org/10.1063/1.4959887

6. *Bruynsteen C., Gehring T., Lupo C., Bauwelinck J., Yin X.* 100-Gbit/s integrated quantum random number generator based on vacuum fluctuations // PRX Quantum. 2023. Vol. 4. N 1. Art. N 010330. https://doi.org/10.1103/PRXQuantum.4.010330

7. *Gehring T., Lupo C., Kordts A., Solar N. D., Jain N., Rydberg T., Pedersen T. B., Pirandola S., Andersen U. L.* Homodyne-based quantum random number generator at 2.9 Gbps secure against quantum side-information // Nature Communications. 2021. Vol. 12. N 1. Art. N 605. https://doi.org/10.1038/s41467-020-20813-w

8. *Drahi D., Walk N., Hoban M. J., Fedorov A. K., Shakhovoy R., Feimov A., Kurochkin Y., Kolthammer W. S., Nunn J., Barrett J., Walmsley I. A.* Certified quantum random numbers from untrusted light // Physical Review X. 2020. Vol. 10. N 4. Art. N 041048. https://doi.org/10.48550/arXiv.1905.09665

9. *Шляйх В. П.* Квантовая оптика в фазовом пространстве / пер. с англ; под ред. В. П. Яковлева. М.: Физматгиз, 2005. 760 с.

10. *Collett M. J., Loudon R., Gardiner C. W.* Quantum theory of optical homodyne and heterodyne detection // Journal of Modern Optics. 1987. Vol. 34. N 6–7. P. 881–902. https://doi.org/10.1080/09500348714550811

11. *Tomamichel M., Schaffner C., Smith A., Renner R.* Leftover hashing against quantum side information // IEEE Transactions on Information Theory. 2011. Vol. 57. N 8. P. 5524–5535. https://doi.org/10.1109/TIT.2011.2158473

12. *Carter J. L., Wegman M. N.* Universal classes of hash functions // Journal of Computer and System Sciences. 1979. Vol. 18. Iss. 2. P. 143–154. https://doi.org/10.1016/0022-0000(79)90044-8

13. *Mansour Y., Nisan N., Tiwari P.* The computational complexity of universal hashing // Theoretical Computer Science. 1993. Vol. 107. P. 121–133. https://doi.org/10.1016/0304-3975(93)90257-T

14. *Ma X., Xu F., Xu H., Tan X., Qi B., Lo H.-K.* Postprocessing for quantum random-number generators: entropy evaluation and randomness extraction // Physical Review A. 2013. Vol. 87. N 6. Art. N 062327. https://doi.org/10.1103/PhysRevA.87.062327

15. *Тихонов В. И., Миронов М. А.* Марковские процессы. М.: Сов. радио, 1977. 488 с.

16. *Абрамовиц М., Стиган И.* Справочник по специальным функциям с формулами, графиками и таблицами. М.: Наука, 1979. 832 с.

17. *Irwin J. O.* The frequency distribution of the difference between two independent variates following the same Poisson distribution // Journal of the Royal Statistical Society. Series A. 1937. Vol. 100. Iss. 3. P. 415–416. https://doi.org/10.1111/j.2397-2335.1937.tb04518.x

18. *Skellam J. G.* The frequency distribution of the difference between two Poisson variates belonging to different populations // Journal of the Royal Statistical Society. Series A. 1946. Vol. 109. Iss. 3. P. 290–296. https://doi.org/10.1111/j.2397-2335.1946.tb04670.x

19. *Vogel V., Grabow J.* Statistics of difference events in homodyne detection // Physical Review A. 1993. Vol. 47. N 5. P. 4227–4235.

20. *Феллер В.* Введение в теорию вероятности и ее приложения. В 2 т. / пер. с англ. Ю. В. Прохорова. М.: Мир, 1984. Т. 2. 738 с.

21. *Haw J. Y., Assad S. M., Lance A. M., Ng N. H. Y., Sharma V., Lam P. K., Symul T.* Maximization of extractable randomness in a quantum random-number generator // Physical Review Appl. 2015. Vol. 3. N 5. Art. N 054004. https://link.aps.org/doi/10.1103/PhysRevApplied.3.054004

22. *Бендат Д., Пирсол А.* Прикладной анализ случайных данных / пер. с англ. В. Е. Привальского, А. И. Кочубинского; под ред. И. Н. Коваленко. М.: Мир, 1989. 540 с.

Статья поступила в редакцию 9 февраля 2024 г.
Статья принята к печати 12 марта 2024 г.

Контактная информация:

Гайдаш Андрей Алексеевич — канд. физ.-мат. наук; andrewdgk@gmail.com

Гончаров Роман Константинович — rkgoncharov@itmo.ru

Козубов Антон Владимирович — канд. физ.-мат. наук; avkozubov@itmo.ru

Яковлев Павел Валентинович — канд. физ.-мат. наук; p.yakovlev@spbu.ru

Mathematical model of random number generator based on vacuum fluctuations

A. A. Gaidash[1], *R. K. Goncharov*[1], *A. V. Kozubov*[1], *P. V. Yakovlev*[2]

[1] University ITMO, 49, Kronversky pr., St. Petersburg, 197101, Russian Federation

[2] St. Petersburg State University, 7–9, Universitetskaya nab., St. Petersburg, 199034, Russian Federation

For citation: Gaidash A. A., Goncharov R. K., Kozubov A. V., Yakovlev P. V. Mathematical model of random number generator based on vacuum fluctuations. *Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes*, 2024, vol. 20, iss. 2, pp. 136–153. https://doi.org/10.21638/spbu10.2024.202 (In Russian)

A mathematical model of quantum random number generator based on vacuum fluctuations is considered. A mathematical justification for the "randomness" of the generated sequence is given under the assumption of the truth of the basic postulates of quantum theory and the validity of the Poisson probability distribution for the photon flux. The results of experiments and the obtained estimates of the minimum entropy are presented.

Keywords: quantum random number generator, minimal entropy estimation, vacuum fluctuations.

References

1. Ermakov S. M. *Metod Monte-Karlo i smezhnye voprosy* [*Monte-Carlo method and related issues*]. Moscow, Nauka Publ., 1975, 472 p. (In Russian)

2. Prokaev A. N. Printsip maksimuma entropii v teorii poiska [The maximum entropy principle in search theory]. *Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes*, 2023, vol. 19, iss. 1, pp. 27–42. https://doi.org/10.21638/11701/spbu10.2023.103 (In Russian)

3. Herrero-Collantes M., Garcia-Escartin J. C. Quantum random number generators. *Rev. Mod. Phys.*, 2023, vol. 89, no. 2, art. no. 015004. https://doi.org/10.1103/RevModPhys.89.015004

4. Gabriel C., Wittmann C., Sych D., Dong R., Mauerer W., Andersen U. L., Marquardt C., Leuchs G. A generator for unique quantum random numbers based on vacuum states. *Nature Photon*, 2010, no. 4, pp. 711–715. https://doi.org/10.1038/nphoton.2010.197

5. Shi Y., Chng B., Kurtsiefer C. Random numbers from vacuum fluctuations. *Applied Physics Letters*, 2016, vol. 109, no. 4, art. no. 041101, pp. 1–5. https://doi.org/10.1063/1.4959887

6. Bruynsteen C., Gehring T., Lupo C., Bauwelinck J., Yin X. 100-Gbit/s integrated quantum random number generator based on vacuum fluctuations. *PRX Quantum*, 2023, vol. 4, no. 1, art. no. 010330. https://doi.org/10.1103/PRXQuantum.4.010330

7. Gehring T., Lupo C., Kordts A., Solar N. D., Jain N., Rydberg T., Pedersen T. B., Pirandola S., Andersen U. L. Homodyne-based quantum random number generator at 2.9 Gbps secure against quantum side-information. *Nature Communications*, 2021, vol. 12, no. 1, art. no. 605. https://doi.org/10.1038/s41467-020-20813-w

8. Drahi D., Walk N., Hoban M. J., Fedorov A. K., Shakhovoy R., Feimov A., Kurochkin Y., Kolthammer W. S., Nunn J., Barrett J., Walmsley I. A. Certified quantum random numbers from untrusted light. *Physical Review X*, 2020, vol. 10, no. 4, art. no. 041048. https://doi.org/10.48550/arXiv.1905.09665

9. Schleich W. P. *Kvatovaya optika v fazovom prostranstve* [*Quantum optics in phase space*]. Moscow, Fizmatgiz Publ., 2005, 760 p. (In Russian)

10. Collett M. J., Loudon R., Gardiner C. W. Quantum theory of optical homodyne and heterodyne detection. *Journal of Modern Optics*, 1987, vol. 34, no. 6–7, pp. 881–902. https://doi.org/10.1080/09500348714550811

11. Tomamichel M., Schaffner C., Smith A., Renner R. Leftover hashing against quantum side information. *IEEE Transactions on Information Theory*, 2011, vol. 57, no. 8, pp. 5524–5535. https://doi.org/10.1109/TIT.2011.2158473

12. Carter J. L. , Wegman M. N. Universal classes of hash functions. *Journal of Computer and System Sciences*, 1979, vol. 18, iss. 2, pp. 143–154. https://doi.org/10.1016/0022-0000(79)90044-8

13. Mansour Y., Nisan N., Tiwari P. The computational complexity of universal hashing. *Theoretical Computer Science*, 1993, vol. 107, pp. 121–133. https://doi.org/10.1016/0304-3975(93)90257-T

14. Ma X., Xu F., Xu H., Tan X., Qi B., Lo H-K. Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction. *Physical Review A*, 2013, vol. 87, no. 6, art. no. 062327. https://doi.org/10.1103/PhysRevA.87.062327

15. Tikhonov V. I., Mironov M. A. *Markovskie processy* [*Markov processes*]. Moscow, Sov. Radio Publ., 1977, 488 p. (In Russian)

16. Abramovitz M., Stegun I. *Spravochnik po spetsialnym aeyrwbzv s formulami, graphikami i tablitsami* [*Handbook of mathematical functions with formulas, graphs, and mathematical tables*]. Moscow, Nauka Publ., 1979, 832 p. (In Russian)

17. Irwin J. O. The frequency distribution of the difference between two independent variates following the same Poisson distribution. *Journal of the Royal Statistical Society*, *Series A*, 1937, vol. 100, iss. 3, pp. 415–416. https://doi.org/10.1111/j.2397-2335.1937.tb04518.x

18. Skellam J. G. The frequency distribution of the difference between two Poisson variates belonging to different populations. *Journal of the Royal Statistical Society*, *Series A*, 1946, vol. 109, iss. 3, pp. 296–296. https://doi.org/10.1111/j.2397-2335.1946.tb04670.x

19. Vogel V., Grabow J. Statistics of difference events in homodyne detection *Physical Review A*, 1993, vol. 47, no. 5, pp. 4227–4235.

20. Feller W. *Vvedenie v teoriyu veroyatnosti i ee prilozheniya* [*An introduction to probability theory and its applications*]. In 2 vol. Moscow, Mir Publ., 1984, vol. 2, 738 p. (In Russian)

21. Haw J. Y., Assad S. M., Lance A. M., Ng N. H. Y., Sharma V., Lam P. K., Symul T. Maximization of extractable randomness in a quantum random-number generator. *Physical Review Appl.*, 2015, vol. 3, no. 5, art. no. 054004. https://link.aps.org/doi/10.1103/PhysRevApplied.3.054004

22. Bendat J. S., Piersol A.G. *Prikladnoy analiz sluchainyh dannyh* [*Random data analysis and measurement procedures*]. Moscow, Mir Publ., 1989, 540 p. (In Russian)

Received: February 9, 2024.
Accepted: March 12, 2024.

Authors' information:

Andrey A. Gaidash — PhD in in Physics and Mathematics; andrewdgk@gmail.com

Roman K. Goncharov — rkgoncharov@itmo.ru

Anton V. Kozubov — PhD in Physics and Mathematics; avkozubov@itmo.ru

Pavel V. Yakovlev — PhD in Physics and Mathematics; p.yakovlev@spbu.ru