ЖЭТФ, 2020, том 157, вып. 3, стр. 442–453

О ФУНДАМЕНТАЛЬНОМ ПРЕДЕЛЕ СКОРОСТИ ГЕНЕРАЦИИ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ В КВАНТОВЫХ ГЕНЕРАТОРАХ С НЕПРЕРЫВНОЙ ПЕРЕМЕННОЙ

С. Н. Молотков*

Институт физики твердого тела Российской академии наук
142432, Черноголовка, Московская обл., Россия

Академия криптографии Российской Федерации
121552, Москва, Россия

Факультет вычислительной математики и кибернетики,
Московский государственный университет им. М. В. Ломоносова
119899, Москва, Россия

Центр квантовых технологий,
Московский государственный университет им. М. В. Ломоносова
119899, Москва, Россия

Поступила в редакцию 16 июля 2019 г.,
после переработки 16 июля 2019 г.
Принята к публикации 1 сентября 2019 г.

Минимальными математическими средствами получено фундаментальное ограничение на скорость генерации случайных чисел в квантовых генераторах случайных чисел с непрерывной переменной. Данное ограничение справедливо при любой интенсивности сигнала — любого числа фотонов в квантовом состоянии. При больших числах заполнения скорость генерации случайных чисел логарифмически растет с увеличением числа фотонов, но всегда остается конечной. При малом числе фотонов скорость генерации пропорциональна числу фотонов. При любом числе фотонов предельная скорость генерации случайных чисел пропорциональна частотной полосе сигнала — квантового состояния.

DOI: 10.31857/S0044451020030050

1. ВВЕДЕНИЕ

Случайные числа и генераторы случайных чисел широко используются в различных областях науки и техники, например, в физике при моделировании методом Монте-Карло. Наиболее широкое применение случайные числа находят в криптографии. В криптографии, в том числе и квантовой, генератор случайных чисел является одним из основных элементов, характеристики которого определяют криптостойкость системы.

В криптографии случайные последовательности используются для генерации секретных ключей в системах симметричного шифрования, генерации паролей, PIN-кодов для различных типов пластиковых карт, кодов аутентификации, вероятностных алгоритмов и систем квантового распределения ключей. Практически для всех упомянутых применений требуются случайные числа, полученные исключительно с физических генераторов.

В квантовой криптографии, которая по сути является процедурой согласования двух независимых случайных последовательностей на передающей и принимающей сторонах посредством посылки и измерения квантовых состояний, требуется очень большой объем случайных чисел. Статистические свойства случайной последовательности и скорость генерации являются главными критериями качества таких генераторов.

В математических генераторах случайных, точнее псевдослучайных, чисел случайная последовательность получается как результат математического преобразования, обычно рекуррентного, некоторого затравочного числа. Любой математический

* E-mail: sergei.molotkov@gmail.com

генератор выдает псевдослучайную последовательность, которая полностью предсказуема, если известны начальные условия — затравочное число.

Физические генераторы основаны на измерении состояния физической системы с дальнейшей экстракцией последовательности 0 и 1 из результатов измерений. При измерении классической системы случайность результата измерения связана только с неизвестностью начальных условий. В этом смысле последовательность результатов измерений является псевдослучайной — полностью определяется, при известном законе эволюции, начальными условиями.

В квантовых генераторах случайных чисел случайность возникает как результат измерения состояния квантовой системы. Эволюция квантовой системы самой по себе также полностью детерминирована, поскольку описывается дифференциальными уравнениями с начальными условиями, но результат измерений принципиально непредсказуем — является случайным, т. е. истинная случайность имеет место только в квантовой области.

Результат измерения над квантовой системой, приготовленной каждый раз в одном и том же начальном условии и испытывающей одну и ту же эволюцию, будет принципиально приводить к непредсказуемому результату. В этом смысле случайность встроена в микромире и возникает как результат измерения.

Принципиально важно уметь экспериментально проверять источник первичной случайности, из которого посредством постобработки возникает случайная последовательность 0 и 1. При разработке генераторов случайных чисел недостаточно того обстоятельства, что тесты на случайность по некоторому статистическому критерию проходят. Это лишь необходимое условие. Принципиально важен источник первичной случайности, который используется для получения равнораспределенной последовательности 0 и 1 и который является действительно источником случайности по соображениям, не зависящим от тестов. Многие генераторы псевдослучайных чисел проходят тесты, но, очевидно, не производят истинно случайных последовательностей. Обзор различных реализаций квантовых генераторов случайных чисел можно найти в работе [1]. Квантовые генераторы случайных чисел можно разделить на две группы.

Первая группа квантовых генераторов случайных чисел в качестве первичной физической случайности использует дискретные фотоотсчеты [2]. Если на физическом уровне достигнута пуассоновская статистика фотоотсчетов, то возможна доказуемая экстракция абсолютно случайной последовательности 0 и 1 [2].

Вторая группа в качестве исходной случайности использует непрерывную случайную величину. Например, такой величиной может быть квадратурная компонента поля при гомодинном детектировании [3]. В последнем случае, по-видимому, приходится делать предположения о статистических свойствах распределения флуктуаций фазы. Исходной случайной величиной для дальнейшего преобразования в последовательность 0 и 1 является разность сигналов с двух классических детекторов, работающих не в режиме счета фотонов, а в линейном режиме. Случайная измеряемая величина возникает как разность токов двух классических фотодетекторов. Поэтому в этом случае сложно контролируемым образом выделить квантовую составляющую сигнала. Например, шум Джонсона – Найквиста довольно трудно, а практически, по-видимому, невозможно контролируемым образом отделить от квантового шума. По этой причине практически невозможно доказать, что источник первичной физической случайности действительно является квантовым. Однако это не самая главная проблема с генераторами случайных чисел с непрерывной переменной как с классическими, так и квантовыми. Существуют фундаментальные ограничения на скорость генерации случайных чисел в таких генераторах.

1. Любой случайный физический процесс — квантовый или классический — имеет спектр на положительной полуоси частот. В этом случае степень убывания корреляций непрерывной случайной величины в разнесенные моменты времени, строго говоря, не может быть даже экспоненциальной, что диктуется фундаментальной теоремой Винера – Пэли [4]. Это означает, что извлекаемые из случайного процесса в разные моменты времени результаты измерений могут оказываться коррелированными (зависимыми). Формально независимыми измерения становятся только при разнесении моментов измерения во времени на бесконечный интервал. В этом случае возникает вопрос: можно ли вообще при таких редких измерениях добиться приемлемой скорости генерации и нужного статистического качества случайных последовательностей?

2. Второй вопрос связан с «мелкостью» дискретизации непрерывной случайной величины. Формально значения непрерывной случайной величины можно дискретизировать со сколь угодно малым масштабом. В этом случае, например, приписывая каждому интервалу случайное число (случай-

ный блок 0 и 1), можно получить за один акт измерения сколь угодно длинный блок случайных 0 и 1 (конечно, с оговорками из предыдущего пункта). Физически очевидно, что масштаб дискретизации измеряемой физической величины, из-за ограничений квантовой механики, не может быть сколь угодно мелким.

Ответам на эти принципиальные вопросы посвящена настоящая работа.

2. МЕТОДЫ ЭКСТРАКЦИИ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Интуитивно понятно, что всякий случайный процесс содержит некоторое максимальное количество истинно случайных 0 и 1. При экстракции случайных битов 0 и 1 из значений случайной величины, получаемой при измерении в физическом процессе, важно знать верхнюю границу этой истинной случайности, для того чтобы гарантировать, что извлекаются истинно случайные, а не коррелированные биты 0 и 1.

Наша задача будет состоять в получении фундаментальной верхней границы скорости экстракции истинной случайности для непрерывной случайной величины в квантовом случае.

Методы извлечения случайности можно разделить на два класса. Первый часто называют универсальным. Универсальные методы экстракции случайности (см., например, [5]) позволяют получить последовательность 0 и 1 сколь угодно близкую к истинно случайной. Мерой близости является следовое расстояние — расстояние Колмогорова между двумя распределениями вероятностей

$$||P_X - P_U||_1 = \frac{1}{2}\sum_{x_i=0,1} |P_X(x_1, x_2, \dots, x_n) - P_U(x_1, x_2, \dots, x_n)| < \varepsilon, \quad (1)$$

$$P_U(x_1, x_2, \dots, x_n) = P_U(x_1)P_U(x_2)\dots P_U(x_n),$$

$$P_U(0) = P_U(1) = \frac{1}{2},$$

где P_X — функция распределения полученной последовательности 0 и 1. Вероятность $P_X(x)$ называется ε-близкой к истинно случайной. Параметр близости ε определяется требованиями по использованию случайных последовательностей. Требуемая близость к идеальной случайной последовательности достигается сжатием (хешированием) при помощи универсальных хеш-функций второго порядка, которые сами являются случайными функциями, что требует затравочной случайности. Такой метод используется, например, для случайных генераторов в [6].

Результаты последовательных актов измерений $(x_1, x_2, \dots, x_n)$ над квантовой системой в общем случае не являются статистически независимыми. Функция распределения не распадается на произведение $P_X(x_1, x_2, \dots, x_n) \neq P(x_1)P(x_2)\dots P(x_n)$. Число истинно случайных битов дается минимальной энтропией Реньи [7]

$$H_{min} = -\log(\max_{P_X(x_1,x_2,\dots,x_n)} P_X(x_1, x_2, \dots, x_n)), \quad (2)$$

ниже везде $\log \equiv \log_2$. Экстракторы позволяют извлечь случайность из распределения $P_X(x_1, x_2, \dots, x_n) \neq P_X(x_1)P_X(x_2)\dots P_X(x_n)$ (см., например, [5–7]).

Однако проблема состоит в том, что в реальной ситуации значения случайной величины в разные моменты измерений коррелированы и, соответственно, функция распределения $P(x_1, x_2, \dots, x_n)$ не есть произведение отдельных независимых функций распределения и неизвестна, поэтому приходится строить предположения, которые трудно экспериментально проверить. И, как следствие, трудно доказать случайность извлекаемых битов 0 и 1.

Вторая группа методов основана на том, чтобы на физическом уровне реализовать такой процесс, который обеспечил бы доказуемую на физическом уровне независимость значений случайной величины в разные моменты времени. Такой подход был реализован в работе [2]. При таком подходе, когда последовательные исходы независимы, $P_X(x_1, x_2, \dots, x_n) = P_X(x_1)P_X(x_2)\dots P_X(x_n)$, минимальная энтропия при $n \to \infty$ переходит в энтропию Шеннона, оценить которую для независимых испытаний можно гораздо проще и надежнее. И главное, для независимых испытаний доказывается, что получаемые биты 0 и 1 действительно являются истинно случайными. При этом алгоритмически с полиномиальной сложностью можно извлечь всю случайность [8], содержащуюся в физическом процессе. Еще одно принципиально важное обстоятельство — при таком подходе не требуется знать сами вероятности $P_X(x_1, x_2, \dots, x_n) = P_X(x_1)P_X(x_2)\dots P_X(x_n)$ при экстракции случайных 0 и 1 [2]. Методы и устройства, использующие данную идеологию, когда алфавит исходной дискретной случайной величины является бинарным (есть фотоотсчет, нет фотоотсчета), были реализованы в работе [2]. Причем методы, использованные в [2], переносятся на дискретную случайную величину с произвольным конечным алфавитом.

3. ДИСКРЕТНЫЙ ИСТОЧНИК БЕЗ ПАМЯТИ ПЕРВИЧНОЙ СЛУЧАЙНОСТИ

Сначала рассмотрим процесс, когда при измерениях над физической системой возникает случайная величина с дискретным алфавитом. Количество истинно случайных битов 0 и 1, которые можно извлечь при n-кратном использовании дискретного случайного источника с алфавитом $\mathcal{X} = \{x_i\}_{i=1}^{M}$ и распределением вероятностей над алфавитом $P_X(x_i)$ при больших n, определяется энтропией Шеннона

$$H(X) = -\sum_{i=1}^{M} P_X(x_i)\log(P_X(x_i)). \tag{3}$$

Число истинно случайных битов 0 и 1 стремится к $nH(X)$ и не превосходит эту величину. Данный факт следует из свойства асимптотической равнораспределенности [9]. Неформально говоря, при $n \to \infty$ имеется $2^{nH(X)}$ типичных последовательностей $x_{i_1}x_{i_2},\ldots,x_{i_n}$, которые асимптотически равновероятны.

В реальной ситуации извлечение случайных битов происходит из конечных блоков первичной последовательности символов x_i, генерируемых физическим источником первичной случайности. Количество истинно случайных битов при условии независимости отдельных исходов в первичной последовательности определяется как

$$H_n(X) = -\sum_{n_{i_1}+n_{i_2}+\ldots+n_{i_M}=n} P_X(x_{i_1})^{n_{i_1}} \times \times P_X(x_{i_2})^{n_{i_2}}\ldots P_X(x_{i_M})^{n_{i_M}} \frac{n!}{n_{i_1}!n_{i_2}!\ldots n_{i_M}!} \times \times \log\left(\frac{n!}{n_{i_1}!n_{i_2}!\ldots n_{i_M}!}\right). \tag{4}$$

Согласно теореме об асимптотической равнораспределенности [9], типичные последовательности имеют вероятность, стремящуюся к единице при больших n. С учетом этого факта, а также используя формулу Стирлинга

$$n! \approx \sqrt{2\pi n}\left(\frac{n}{e}\right)^n, \tag{5}$$

в главном приближении имеем

$$\frac{n!}{n_{i_1}!n_{i_2}!\ldots n_{i_M}!} \to \frac{n^n}{(P_X(x_1)n)^{P_X(x_1)n}(P_X(x_2)n)^{P_X(x_2)n}\ldots(P_X(x_M)n)^{P_X(x_M)n}}. \tag{6}$$

Поскольку

$$\sum_{k=1}^{M} P_X(x_k) = 1, \tag{7}$$

с учетом (4)–(6) находим

$$H_n(X) \to \log\left(\frac{n^n}{(P_X(x_1)n)^{P_X(x_1)n}(P_X(x_2)n)^{P_X(x_2)n}\ldots(P_X(x_M)n)^{P_X(x_M)n}}\right) = = -n\sum_{i=1}^{M} P_X(x_i)\log(P_X(x_i)) = nH(X), \tag{8}$$

где i_k — номер позиции k-го элемента алфавита. Формула (8) имеет простую интерпретацию. Число последовательностей, которые содержат n_{i_1} символов x_{i_1}, n_{i_2} символов x_{i_2} и т. д., равно биномиальному коэффициенту (второй сомножитель под знаком суммы), величина которого есть число способов размещения элементов в строке длиной n.

Первый сомножитель — это вероятность появления каждой последовательности с данным числом каждого символа. При больших n величина $H_n(X) \to nH(X)$, это следует из формулы Стирлинга (5) и того факта, что число появлений каждого символа в асимптотическом пределе $n_{i_k} \to nP_X(x_{i_k})$, и соответственно вероятность появления стремится к $P_X(x_{i_k})^{nP_X(x_{i_k})}$. Как следствие, получаем формулу (8).

Дальнейшая задача состоит в экстракции случайных битов из блоков последовательностей длиной n, генерируемых источником с дискретным алфавитом и представляющих собой первичную случайность.

Все последовательности с одинаковым количеством каждого символа, различающиеся лишь порядком символов, являются равновероятными. Все множество последовательностей разбивается на классы равновероятных последовательностей, каждый класс отвечает определенному разбиению $n = n_{i_1} + n_{i_2} + \ldots + n_{i_M}$ $(n_{i_k} = 0, 1, \ldots, n,\ k = 1, 2, \ldots, M)$. После нумерации всех последовательностей в каждом классе, точнее, бинарное представление номера последовательности в классе дает блок истинно случайных битов 0 и 1 (см. детали в [8] и в [2]). Возможен эффективный способ извлечения истинно случайных битов при условии независимости исходных символов [8], который был реализован в устройствах [2].

В заключение данного раздела можно резюмировать: мерой и верхней границей истинной случайности в случае источника с дискретным алфавитом является энтропия Шеннона, причем данная верхняя граница конструктивно достижима с полиномиальными вычислительными ресурсами по длине первичной последовательности.

4. ДИФФЕРЕНЦИАЛЬНАЯ ЭНТРОПИЯ НЕПРЕРЫВНОЙ СЛУЧАЙНОЙ ВЕЛИЧИНЫ

Принципиально иная ситуация возникает при извлечении истинно случайных битов 0 и 1 из непрерывной случайной переменной. Как правило, в реальности непрерывная случайная величина возникает при наблюдении физического процесса, зависящего от времени. В каждый момент времени t измерение дает значение случайной физической величины $x(t)$. Для того чтобы обозначить суть проблемы при работе с непрерывной переменной, рассмотрим для начала случайную величину x в некоторый фиксированный момент времени t, индекс t пока опустим.

Аналогом энтропии Шеннона для дискретного источника без памяти, которая служит мерой количества информации (случайности), содержащейся в дискретной случайной величине, в случае непрерывной случайной величины $x \in (-\infty, \infty)$ с функцией плотности распределения вероятности $p(x)$, является дифференциальная энтропия [9]. По определению имеем

$$H(p) = -\int\limits_{-\infty}^{\infty} p(x)\, d\log(p(x)). \tag{9}$$

Если не вводить никаких дополнительных ограничений на случайную переменную x, то сделать какие-то содержательные утверждения часто невозможно. Поскольку любой реализуемый физический сигнал, при наблюдении которого возникает случайная переменная x, имеет конечную мощность, то естественным ограничением является ограниченность величины «мощности», имеем

$$\int\limits_{-\infty}^{\infty} x^2 p(x)\, dx \le \sigma^2. \tag{10}$$

При этом максимум дифференциальной энтропии (9) достигается на гауссовском распределении [9,10]

$$p(x) = \frac{1}{\sqrt{2\pi}\sigma} \exp\left(-\frac{x^2}{2\sigma^2}\right).$$

В этом случае для дифференциальной энтропии (9) получаем

$$H(p) = \frac{1}{2}\log(2\pi e\sigma^2). \tag{11}$$

Если в случае дискретного источника, как было показано выше, энтропия Шеннона является мерой истинной случайности, содержащейся в источнике, то в случае непрерывной случайной величины ситуация сложнее.

Дифференциальная энтропия не является прямой мерой истинной случайности, которую можно извлечь из источника случайного непрерывного сигнала. Более того, дифференциальная энтропия может быть даже отрицательной.

В дальнейшем нас будут интересовать фундаментальные ограничения на скорость извлечения истинно случайных битов 0 и 1 из непрерывного случайного сигнала.

В классической области любая величина может быть измерена со сколь угодно большой точностью. Классическая физика не накладывает никаких фундаментальных ограничений на точность измерения. Это означает, что интервал изменений непрерывной случайной классической величины может быть дискретизирован на сколь угодные малые интервалы Δ. Дискретизация превращает непрерывную случайную величину в дискретную случайную величину X_Δ.

Дискретизация состоит в следующем. При измерении непрерывной случайной величины весь диапазон значений разбивается на интервалы Δ, при этом функция распределения становится равной

$$\Delta p(x_i) = \int\limits_{i\Delta}^{(i+1)\Delta} p(x)\, dx, \tag{12}$$

где x_i — «средняя» точка в интервале $(i\Delta,(i+1)\Delta)$. В результате дискретизации энтропия принимает вид

$$H(X_\Delta) = -\sum_i \Delta p(x_i)\log(p(x_i)) - \log\Delta, \qquad (13)$$

при $\Delta\to 0$ имеем $\sum_i \Delta p(x_i)\log(p(x_i)) \to H(p)$, тогда энтропия

$$H(X_\Delta) = H(p) - \log\Delta. \qquad (14)$$

Для гауссовского сигнала после дискретизации энтропия становится равной

$$H(X_\Delta) = \frac{1}{2}\log\frac{2\pi e\sigma^2}{\Delta}. \qquad (15)$$

После дискретизации могут быть использованы методы экстракции истинно случайных 0 и 1, описанные выше. Но при этом, при $\Delta\to 0$, энтропия дискретного источника (14), (15) стремится к бесконечности.

Это означает, что за один акт измерения можно получить сколь угодно много случайных битов 0 и 1.

Действительно, разобьем диапазон изменений непрерывной случайной величины на интервалы таким образом, чтобы вероятности попадания в каждый интервал были одинаковыми. Припишем каждому интервалу его номер в лексикографическом порядке, начиная с 0. Бинарное представление номера и будет случайным блоком 0 и 1. Очевидно, что при стремлении масштаба дискретизации к нулю, $\Delta\to 0$, за один акт измерения можно получить сколь угодно большой блок истинно случайных 0 и 1, что является явным абсурдом.

Для того чтобы устранить данное противоречие здравому смыслу, обычно говорятся слова, что процесс измерений сам вносит шум, поэтому интервал дискретизации нельзя выбирать меньше амплитуды шума.

Такое заметание проблемы «под ковер» не является решением. Да и с логической точки зрения такой подход абсурден, поскольку измеряется общее значение переменной, которое содержит вклад от всех процессов, а процесс дискретизации является внешним. Грубо говоря, количество извлекаемой случайности зависит от «волевого решения по дискретизации», поэтому невозможно всерьез говорить о случайности извлекаемых битов 0 и 1.

Ясно, что любой физический сигнал нельзя дискретизировать до бесконечности в сторону уменьшения интервала Δ. На каком-то этапе неизбежно возникнут ограничения, диктуемые квантовой природой сигнала, причем независимо от его интенсивности. Фигурально говоря, нельзя дискретизировать сигнал до масштабов, меньших отдельного фотона. Любой интенсивный сигнал, хоть и содержит макроскопически большое число фотонов, но все же конечное.

Кратко резюмируем сказанное — квантовая природа микромира должна ограничивать степень дискретизации, что неизбежно должно приводить к конечности энтропии сигнала, соответственно, накладывать фундаментальные ограничения на скорость экстракции истинно случайных битов 0 и 1.

Для того чтобы выяснить фундаментальные ограничения на скорость экстракции случайных битов, необходимо сразу рассматривать сигнал как квантовый — квантовое состояние, которое может содержать любое число фотонов.

Следующая проблема, которая возникает при экстракции случайных битов из непрерывного случайного классического или квантового сигнала, состоит в следующем. Измерения над сигналом $x(t)$ проводится, как правило, через определенные промежутки времени τ. Обычно выбирается стационарный случайный процесс. Для того чтобы блоки случайных битов 0 и 1, извлекаемых из непрерывной случайной величины в момент t_i и момент $t_{i\pm1}$, были независимыми, значения непрерывной случайной величины $x(t_i)$ и $x(t_{i\pm1})$ тоже должны быть статистически независимыми. В противном случае случайные биты, полученные в разные моменты времени, будут зависимыми (коррелированными), т. е. не будут случайными.

Для стационарного процесса степень корреляции случайной величины в разные моменты времени $x(t_i)$ и $x(t_{i\pm1})$ определяется корреляционной функцией, зависящей только от разности моментов времени [10]:

$$\mathcal{K}(\tau) = \mathbf{E}[x(t)x(t+\tau)]. \qquad (16)$$

Интуитивно ясно, что чем больше частотная полоса сигнала $x(t)$, тем быстрее убывают корреляции между значениями сигнала во времени. Чем быстрее убывают корреляции в моменты t и $t+\tau$, тем большей скорости генерации случайных чисел можно достичь при измерении $x(t)$ через меньшие интервалы времени τ. Однако и здесь возникают фундаментальные ограничения, которые имеют место как в классическом, так и квантовом случаях (см. ниже).

Любой физический сигнал имеет спектр на положительной полуоси частот ω, т. е. $\omega\in[0,\infty)$, что приводит к фундаментальным ограничениям на скорость уменьшения корреляционной функции $\mathcal{K}(\tau)$ во времени. Согласно теореме Винера – Пэли [4], для

любой квадратично интегрируемой функции по времени (имеющей конечный интеграл, в нашем случае $\mathcal{K}(\tau)$), имеющей спектр на полуоси ($\mathcal{K}(\omega)$, $\omega \in [0,\infty)$), следующий интеграл должен сходиться (быть меньше бесконечности):

$$\int\limits_{-\infty}^{\infty} \frac{|\log(\mathcal{K}(\tau))|}{1+\tau^2}\, d\tau < \infty. \tag{17}$$

Из формулы (17) следует, что коррелятор $\mathcal{K}(\tau)$ не может уменьшаться даже экспоненциально. Экспоненциальное убывание ($\propto e^{-\tau}$) приводило бы к логарифмической расходимости интеграла в (17). Хотя убывание, сколь угодно близкое к экспоненциальному, не запрещается (см. ниже).

Данное ограничение действительно является фундаментальным и возникает во многих физических ситуациях. Например, степень локализуемости безмассового квантового поля фотонов также регулируется теоремой Винера – Пэли [4] (см. детали в работе [11]).

Идеальной ситуация для скорости экстракции случайных чисел была бы, если бы коррелятор был δ-функционным:

$$\mathcal{K}(\tau) \propto \delta(\tau). \tag{18}$$

В этом случае можно было бы измерять значение случайной величины через сколь угодно малые временные интервалы. Однако для такого поведения коррелятора спектр должен быть равномерным на всей оси частот, включая отрицательные частоты, $\omega \in (-\infty,\infty)$, что для физической системы невозможно. Спектр может быть только на положительной полуоси. Даже для равномерного спектра на полуоси, $\mathcal{K}(\omega) \propto \theta(\omega)$, временное поведение коррелятора имеет вид

$$\mathcal{K}(\tau) \propto \delta(\tau) + \frac{1}{\pi}\mathrm{PV}\frac{i}{\tau}, \tag{19}$$

т. е. коррелятор становится обобщенной функцией, которая имеет степенные хвосты.

Поскольку любое измерительное устройство имеет эффективно ограниченную частотную полосу, математически удобнее формулировать задачу следующим образом (и, по-видимому, это единственная формулировка, при которой можно получить надежные результаты). Для того чтобы явно не вводить в рассмотрение измерительное устройство, удобно считать, что сам физический сигнал имеет конечную частотную полосу $\omega \in [0,\Omega]$ (положение на оси частот, как увидим ниже, не важно, можно всегда сдвинуть интервал частот в нужное положение). Далее, пусть время наблюдения сигнала ограничено интервалом $[0,T]$ и пусть вне этого интервала сигнал исчезающе мал (точное условие малости см. ниже). Пусть источник непрерывного сигнала выдает только такие сигналы, которые имеют ограниченную частотную полосу и локализованы, насколько это допустимо природой, во временном окне $[0,T]$.

Если источник может генерировать N ортогональных состояний с такими свойствами и число таких состояний ограничено (конечно), то при равновероятной генерации состояний будет достигаться максимальная энтропия, величина которой и будет определять скорость генерации случайных чисел. Ортогональность состояний нужна для их различимости.

5. БАЗИСНЫЕ ФУНКЦИИ — ВОЛНОВЫЕ ФУНКЦИИ ВЫТЯНУТОГО СФЕРОИДА

Перейдем к более точным формулировкам. Возможны два способа представления сигналов с ограниченным частотным спектром как функции времени. Первый способ основан на фундаментальной теореме В. А. Котельникова об отсчетах [12]. Сигнал с конечным частотным спектром и почти локализованный во временном окне $[0,T]$ представляется в виде разложения в ряд по отсчетным функциям, которые играют роль базисных функций. Для случайного процесса $x(t)$ имеем

$$x(t) = \sum_{-\infty}^{\infty} x\left(\frac{2\pi n}{\Omega}\right) \frac{\sin\left[\Omega\left(t-\dfrac{2\pi n}{\Omega}\right)\right]}{\Omega\left(t-\dfrac{2\pi n}{\Omega}\right)}, \tag{20}$$

где значения сигнала $c_n = x\left(2\pi n/\Omega\right)$ в отсчетные моменты $t_n = 2\pi n/\Omega$ являются случайными непрерывными величинами. Для случайного сигнала с ограниченным спектром, и приближенно ограниченного по времени, в разложении остаются только $N = \Omega T$ слагаемых.

Второй способ описания состоит в выборе функций с ограниченным спектром, максимально локализованных в окне $]0,T]$, в качестве базисных функций. Коэффициенты разложения сигнала по этим функциям будут играть роль непрерывных случайных величин. Число таких ортогональных функций, локализованных почти целиком в окне $]0,T]$, также равно $N = \Omega T$.

Оба подхода приводят к одинаковым результатам, так как число независимых степеней свободы в сигнале одинаково и определяется параметром $N = \Omega T$. Мы выберем второй способ, поскольку он

более удобен при описании ситуации в квантовом случае. В классическом случае сигнал измеряется в отсчетные моменты. В квантовом случае измерение в том или ином виде является проектированием на определенное квантовое состояние, поэтому (см. ниже) второй способ более удобен в этом случае.

Условие максимальной локализации сигнала во временном окне $[0,T]$

$$\max_{\omega\in[0,\Omega]}\int\limits_0^T x^2(t)\,dt \tag{21}$$

приводит к известному интегральному уравнению для (см. детали в [13–15])

$$\lambda_n(c)\varphi_n(t,c)=\frac{1}{\pi}\int\limits_0^T\frac{\sin[\Omega(t-t')]}{t-t'}\varphi_n(t',c)\,dt', \tag{22}$$

$$2c=\Omega T.$$

Решением являются замечательные функции, называемые волновыми функциями вытянутого сфероида [13–15]. Данные функции возникают в ряде задач математической физики.

При разных n и n' функции ортогональны как на конечном $[0,T]$, так и на бесконечном $(-\infty,\infty)$ интервалах,

$$\begin{aligned}&\int\limits_0^T\varphi_n(t,c)\varphi_{n'}(t,c)\,dt=\lambda_n(c)\delta_{n,n'},\\ &\int\limits_{-\infty}^{\infty}\varphi_n(t,c)\varphi_{n'}(t,c)\,dt=\delta_{n,n'}.\end{aligned} \tag{23}$$

Забегая вперед, скажем, что ортогональность как на конечном, так и на бесконечном интервалах позволяет совершить аккуратный предельный переход к бесконечности, когда временное окно наблюдения $T\to\infty$. Свойство ортогональности при предельном переходе сохраняет свойство различимости базисных состояний.

Степень локализации во временном окне $[0,T]$ собственной функции с номером n уравнения (22) дается ее собственным числом:

$$\int\limits_0^T\varphi_n^2(t,c)\,dt=\lambda_n(c). \tag{24}$$

Замечательным свойством волновых функций вытянутого сфероида является их поведение в зависимости от величины параметра ΩT. При $\Omega T\gg 1$ имеется $N=\Omega T$ функций, которые локализованы во временном окне с субэкспоненциальной точностью (качественная иллюстрация этого свойства приведена на рис. 1, см. детали в [13,14]),

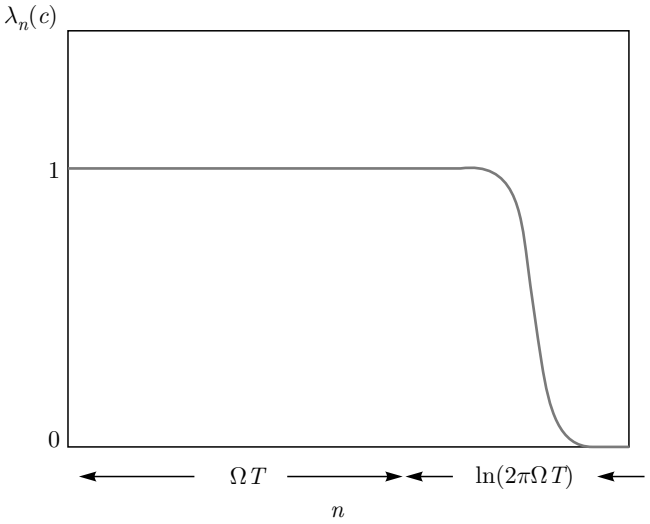

Рис. 1. Качественная иллюстрация поведения собственных чисел в зависимости от номера собственного числа

$$\lambda_n(c)\sim 1-\frac{4\sqrt{\pi}8^n c^{n+1/2}}{n!}e^{-c},\quad c=\Omega T. \tag{25}$$

Как видно из (25), степень локализации собственных значений при заданном номере n является субэкспоненциальной от временного окна T из-за множителя $c^{n+1/2}$ перед экспонентой. Имеется примерно $\log(\Omega T)$ функций в переходной области (см. рис. 1), остальные почти равны нулю в окне $[0,T]$.

Принципиальным фактом при использовании в качестве базисных функций вытянутого сфероида является следующий результат [13,14]. Для любого $\varepsilon>0$ имеют место равенства

$$\lim_{\Omega T\to\infty}\lambda_{\Omega T(1-\varepsilon)}=1,\quad \lim_{\Omega T\to\infty}\lambda_{\Omega T(1+\varepsilon)}=0. \tag{26}$$

Неформально это означает, что имеется ΩT номеров функций, которые почти целиком локализованы во временном окне T. Для остальных номеров функции равны нулю (при этом они остаются нормированными, нормировка набирается на всем бесконечном интервале). Переходная область по номерам имеет масштаб $\sim\ln(2\pi\Omega T)$, т. е. является крайне узкой — логарифмически узкой по сравнению с ΩT.

6. ДИФФЕРЕНЦИАЛЬНАЯ ЭНТРОПИЯ НЕПРЕРЫВНОГО СИГНАЛА С КОНЕЧНЫМ ЧАСТОТНЫМ СПЕКТРОМ

Сигналы, для наблюдения которых требуется время T, могут быть представлены как

$$x(t)=\sum_{n\le N} c_n\overline{\varphi}_n(t),\quad \overline{\varphi}_n(t)=\frac{1}{\sqrt{\lambda_n(c)}}\varphi_n(t), \quad (27)$$

где c_n является случайной величиной. Дифференциальная энтропия сигнала при наблюдении во временном окне $[0,T]$

$$H(x)_T=-\sum_{n=1}^{N} H(c_n), \quad (28)$$

где $H(c_n)$ — энтропия n-й моды. При ограничении на мощность сигнала

$$\sum_{n=1}^{N} c_n^2\le\sigma^2 N \quad (29)$$

максимум дифференциальной энтропии достигается для гауссовского распределения c_n, имеем

$$H(X)=\frac{1}{2}N\sum_{n=1}^{N}\log(2\pi e\sigma^2). \quad (30)$$

Опять при неограниченно мелкой дискретизации интервала изменений значений непрерывной случайной величины энтропия становится равной

$$H(X_\Delta)=\frac{1}{2}N\sum_{n=1}^{N}\log\frac{2\pi e\sigma^2}{\Delta}. \quad (31)$$

Соответственно скорость генерации дифференциальной энтропии в единицу времени равна

$$\lim_{\Omega T\to\infty} H(X_\Delta)_T=\lim_{\Omega T\to\infty}\frac{H(X_\Delta)}{T}= \\ =\frac{1}{2}\Omega\sum_{n=1}^{N}\log\frac{2\pi e\sigma^2}{\Delta}. \quad (32)$$

Отсюда видно, что энтропия неограниченно возрастает с уменьшением Δ. Из формулы (32) видно, что устранение проблемы с локализацией сигнала не решает проблему с дискретизацией. Проблему дискретизации невозможно логически последовательно решить в классической области, для этого нужно квантовое рассмотрение сигнала с самого начала.

7. КВАНТОВЫЙ СЛУЧАЙ

Будем рассматривать квантовые состояния с ограниченным частотным спектром Ω. Пусть квантовое состояние поля содержит M фотонов — бозе-частиц. Состояние имеет носитель в конечной частотной полосе Ω. В качестве одночастичных базисных состояний выберем волновые функции вытянутого сфероида $\varphi_n(\omega)$. Таких функций $N=\Omega T$. Число многочастичных ортогональных векторов состояний с M фотонами, локализованных во временном окне T, равно числу способов размещения M фотонов по N одночастичным состояниям. Число размещений бозе-частиц по N состояниям равно [16]

$$C_{N-1+M}^{M}=\frac{(N-1+M)!}{(N-1)!M!}. \quad (33)$$

Вектор состояния, отвечающий размещению — разбиению числа $n_1+n_2+\ldots+n_N=M$, имеет вид

$$|\Phi_{n_1,n_2,\ldots,n_N}\rangle=\int\limits_{\Omega}\ldots\int\limits_{\Omega} d\omega_1 d\omega_2\ldots d\omega_{n_1}\ldots d\omega_{n_1+1}\times \\ \times d\omega_{n_1+2}\ldots d\omega_{n_2}, d\omega_{n_{N-1}+1}d\omega_{n_{N-1}+2}\ldots d\omega_{n_N}\times \\ \times\varphi_1(\omega_1)\varphi_1(\omega_2)\ldots\varphi_1(\omega_{n_1})\varphi_2(\omega_{n_1+1})\times \\ \times\varphi_2(\omega_{n_1+2})\ldots\varphi_2(\omega_{n_2})\ldots\varphi_N(\omega_{n_{N-1}+1})\times \\ \times\varphi_N(\omega_{n_{N-1}+2})\ldots\varphi_N(\omega_{n_N})\times \\ \times|\omega_1,\omega_2,\ldots,\omega_{n_1},\ldots,\omega_{n_1+1},\omega_{n_1+2},\ldots,\omega_{n_2}, \\ \omega_{n_{N-1}+1},\omega_{n_{N-1}+2},\ldots,\omega_{n_N}\rangle. \quad (34)$$

Дальнейшая логика рассуждений следующая. При заданном числе фотонов в состоянии M имеется C_{N-1+M}^{M} (33) ортогональных, а значит, достоверно различимых квантовых состояний на интервале $[0,T]$, которые локализованы почти целиком в этом окне. Измерения во временном окне позволяют различить все ортогональные состояния. Максимальная энтропия источника достигается в том случае, когда источник генерирует все C_{N-1+M}^{M} ортогональных различимых состояний равновероятно. Такой источник описывается матрицей плотности — квантовым ансамблем

$$\rho(N,M)=\frac{1}{C_{N-1+M}^{M}}\times \\ \times\sum_{n_1+n_2+\ldots+n_N=M}|\Phi_{n_1,n_2,\ldots,n_N}\rangle\langle\Phi_{n_1,n_2,\ldots,n_N}|. \quad (35)$$

Измерение над квантовыми состояниями, генерируемыми источником, которое позволяет различить все ортогональные состояния, локализованные во временном окне $[0,T]$, дается следующим разложением единицы:

$$I_{N,M} = \sum_{n_1+n_2+\ldots+n_N=M} \mathcal{P}_T(n_1,n_2,\ldots,n_N) + \\ + I^{\perp}_{N,M}, \quad (36)$$
$$I^{\perp}_{N,M} = \sum_{n_1+n_2+\ldots+n_N=M} \mathcal{P}_{\perp}(n_1,n_2,\ldots,n_N),$$

где

$$\mathcal{P}_T(n_1,n_2,\ldots,n_N) = |\overline{\Phi}_{n_1,n_2,\ldots,n_N}\rangle\langle\overline{\Phi}_{n_1,n_2,\ldots,n_N}|$$

— проектор на квантовое состояние, локализованное во временном окне $[0,T]$; $I^{\perp}_{N,M}$ — дополнение до полного пространства состояний на всей временной оси;

$$\mathcal{P}_{\perp}(n_1,n_2,\ldots,n_N) = |\perp_{n_1,n_2,\ldots,n_N}\rangle\langle\perp_{n_1,n_2,\ldots,n_N}|$$

— проектор на состояния, описывающие хвосты волновых функций вытянутого сфероида вне окна $[0,T]$.

Для вероятности исходов с учетом (36) получаем

$$\begin{aligned} &P_T(n_1,n_2,\ldots,n_N) = \\ &= \mathrm{Tr}\{\mathcal{P}_T(n_1,n_2,\ldots,n_N)\rho(N,M)\} = \\ &\qquad = \frac{\lambda_N(n_1,n_2,\ldots,n_N)}{C^M_{N-1+M}}, \\ &P_{\perp}(n_1,n_2,\ldots,n_N) = \\ &= \mathrm{Tr}\{\mathcal{P}_{\perp}(n_1,n_2,\ldots,n_N)\rho(N,M)\} = \\ &\qquad = \frac{1-\lambda_N(n_1,n_2,\ldots,n_N)}{C^M_{N-1+M}}. \end{aligned} \quad (37)$$

В каждом акте измерения во временном окне $[0,T]$ возникает случайно один из C^M_{N-1+M} исходов (37). Соответственно для энтропии фон Неймана источника, которая для ортогональных состояний совпадает с энтропией Шеннона, получаем

$$\begin{aligned} H(mT,\Omega T) = H(N,M) = \\ = -\sum_{n_1+n_2+\ldots+n_N=M} \frac{\lambda_N(n_1,n_2,\ldots,n_N)}{C^M_{N-1+M}} \times \\ \times \log\left(\frac{\lambda_N(n_1,n_2,\ldots,n_N)}{C^M_{N-1+M}}\right) - \\ - \sum_{n_1+n_2+\ldots+n_N=M} \frac{1-\lambda_N(n_1,n_2,\ldots,n_N)}{C^M_{N-1+M}} \times \\ \times \log\left(\frac{1-\lambda_N(n_1,n_2,\ldots,n_N)}{C^M_{N-1+M}}\right), \end{aligned} \quad (38)$$

где

$$\lambda_N(n_1,n_2,\ldots,n_N) = \lambda_1^{n_1}(N)\lambda_2^{n_2}(N)\ldots\lambda_N^{n_M}(N).$$

Вклад в энтропию за счет исходов измерений вне окна $[0,T]$ не превосходит величину последнего слагаемого в (38) и стремится к нулю в пределе $\Omega T \to \infty$.

Отметим, что энтропия в (38) — это просто энтропия Шеннона, а не дифференциальная энтропия. Напомним (см. разделы выше), что именно энтропия Шеннона определяет число истинно случайных битов 0 и 1, которые можно извлечь при измерениях.

Поскольку $N \gg 1$, воспользовавшись формулой Стирлинга (5) для значения факториала в главном приближении, получаем

$$C^M_{N-1+M} \approx \frac{(N+M)^N(N+M)^M}{N^N M^M} = \\ = \left(1+\frac{M}{N}\right)^N \left(1+\frac{N}{M}\right)^M, \quad (39)$$

где M — число фотонов во временном окне $[0,T]$. Удобно для дальнейшего ввести обозначение $M = mT$, где m имеет смысл числа фотонов в единицу времени и имеет такую же размерность, как частота Ω [1/с], поэтому отношение m/Ω является безразмерным.

С учетом (38), (39) находим, что энтропия, генерируемая источником в единицу времени, равна

$$H(m,\Omega) = \lim_{\Omega T\to\infty} \frac{H(mT,\Omega T)}{T} = \\ = \Omega\left[\log\left(1+\frac{m}{\Omega}\right) + \frac{m}{\Omega}\log\left(1+\frac{\Omega}{m}\right)\right], \quad (40)$$

где отношение m/Ω имеет смысл числа фотонов в единичной частотной полосе.

Рассмотрим асимптотики (40) при различных числах фотонов в состоянии. При малом числе фотонов — предельно квантовый сигнал, $m/\Omega \ll 1$, выражение для скорости генерации энтропии принимает вид

$$H(m,\Omega) \approx \Omega\left(\frac{m}{\Omega}\right) = m, \quad (41)$$

и она пропорциональна числу фотонов в единичную частотную полосу. Скорость генерации энтропии фактически определяется частотной полосой сигнала (или измеряющего устройства, см. замечание выше). Формально ширина частотной полосы в формуле (41) сокращается, скорость генерации энтропии пропорциональна числу фотонов, но отсюда не следует, что отсчеты можно делать с любой скоростью — малым временным интервалом между отсчетами.

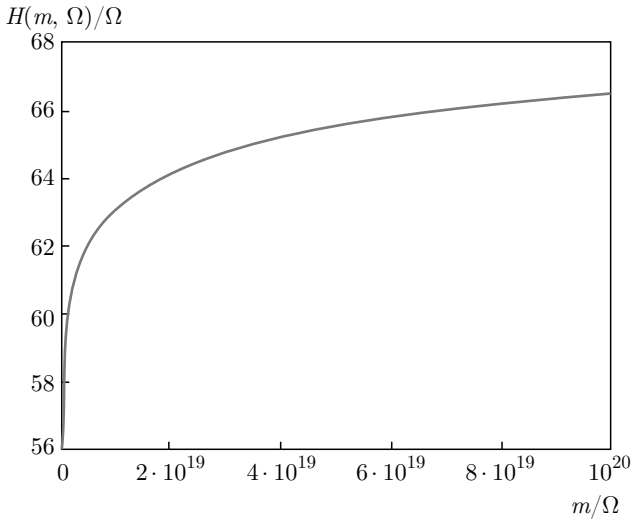

Рис. 2. Предельная скорость генерации случайных битов как функция числа фотонов в единичной полосе частот

При большом числе фотонов, $m/\Omega \gg 1$ — классический предел, второе слагаемое в правой части (40) остается конечным и стремится к

$$\frac{m}{\Omega}\log\left(1+\frac{\Omega}{m}\right) \to \frac{1}{\ln 2}, \quad \frac{m}{\Omega} \to \infty. \tag{42}$$

Первое слагаемое в (40) логарифмически растет с увеличением числа фотонов (интенсивности сигнала):

$$H(m,\Omega) \approx \Omega \log\left(1+\frac{m}{\Omega}\right). \tag{43}$$

Единица в формуле (43) под логарифмом оставлена специально для дальнейших обсуждений ниже. В итоге энтропия источника в единицу времени — скорость генерации истинно случайных битов, растет логарифмически с увеличением числа фотонов (мощности сигнала), но при этом остается конечной. Подчеркнем, во избежание недоразумений, что данная величина энтропии достигается, если над квантовым состоянием, содержащим большое число фотонов, проводится действительно квантовое измерение, которое позволяет различать разные компоненты в квантовом ансамбле (35).

Скорость генерации энтропии как в квантовом пределе малого числа фотонов, так и в пределе большого числа фотонов остается пропорциональной частотной полосе сигнала Ω.

Для иллюстрации зависимость скорости генерации энтропии — скорости генерации случайных битов — как функции числа фотонов (интенсивности) представлена на рис. 2.

Формулы (40)–(43) относятся к случаю, когда число фотонов задано. Если в состоянии задано лишь среднее число фотонов как, например, в когерентном состоянии, то формула (40) для скорости генерации переходит в следующую:

$$H(\mu_\Omega,\Omega) = \Omega\sum_{k=0}^{\infty} e^{-\mu_\Omega}\frac{(\mu_\Omega)^k}{k!}H(k,\Omega). \tag{44}$$

Здесь μ_Ω — среднее число фотонов в единичной частотной полосе, $H(k,\Omega)$ — парциальная энтропия состояния с k фотонами, см. (40), где нужно заменить $m/\Omega \to k$.

8. ОБСУЖДЕНИЕ РЕЗУЛЬТАТОВ

Полезно обсудить связь полученных результатов для квантового случая с известными результатами в классической области. Обратимся к формуле (43), которая структурно похожа на классическую формулу Шеннона [17] для пропускной способности (C) классического канала с информационным сигналом с конечным спектром (Ω) и гауссовским шумом в канале,

$$C = \Omega \log\left(1+\frac{P_\Omega}{P_{noise}}\right). \tag{45}$$

Здесь P_Ω/P_{noise} — известное отношение сигнал–шум, P_Ω — мощность сигнала в единичной полосе частот, P_{noise} — мощность шума в канале в единичной полосе частот. При стремлении мощности шума к нулю пропускная способность переходит в энтропию источника (передатчика) и стремится к бесконечности. То есть без шума канал с непрерывной переменной позволяет в классическом случае передать сколь угодно большое количество информации в единицу времени. Этот факт есть отражение проблемы дискретизации непрерывной случайной величины, которая обсуждалась выше.

По этой причине часть исследователей из-за неверной интерпретации классической формулы (45) ошибочно считают, что шум играет фундаментальную роль при описании каналов с непрерывной переменной. Кстати, ничего подобного в работах основателей теории информации никогда не утверждалось. Введение шума, скорее, является техническим приемом. Правильный ответ состоит в том, что проблема дискретизации не имеет последовательного решения в классической области. Естественное разрешение проблемы возникает при квантовом рассмотрении источника, при этом энтропия (см. формулу (40)), соответственно, пропускная способность остаются всегда конечными даже в отсутствие шума. Не следует «тянуть» классическое описание в ту область, где оно перестает работать.

Вернемся к обсуждению генерации случайных чисел в квантовых генераторах с непрерывной переменной. Во многих работах (см. ссылки в обзоре [1]) декларируются высокие скорости генерации случайных чисел в квантовых генераторах с непрерывной переменной. В большинстве случаев такие генераторы основаны на гомодинном детектировании флуктуаций вакуума. Например, в работе [18] скорость генерации первичной случайности достигала почти 480 Мбит/с при эффективной частотной полосе квантовых флуктуаций $\Omega \approx 150$ МГц, что явно превышает теоретический предел. По этой причине случайные последовательности на выходе такого генератора вряд ли можно признать истинно случайными.

Благодарности. Автор выражает благодарность И. М. Арбекову и С. П. Кулику за интересные и многочисленные обсуждения, а также коллегам по Академии криптографии Российской Федерации за обсуждения и поддержку.

Финансирование. Работа поддержана Российским научным фондом (грант №16-12-00015 (П)).

ЛИТЕРАТУРА

1. M. Herrero-Collantes and J. Carlos Garcia-Escartin, Rev. Mod. Phys. **89**, 015004 (2017).

2. К. А. Балыгин, В. И. Зайцев, А. Н. Климов, С. П. Кулик, С. Н. Молотков, ЖЭТФ **153**, 879 (2018).

3. Q. Zhou, R. Valivarthi, C. John, and W. Tittel, arXiv: 1703.00559 (2017).

4. Н. Винер, Р. Пэли, *Преобразование Фурье в комплексной области*, Наука, Москва (1964).

5. L. Trevisan, J. ACM **48**, 860 (2001).

6. W. Mauerer, C. Portmann, and V. B. Scholz, arXiv: 1212.0520 (2012).

7. R. König, R. Renner, and C. Schaffner, IEEE Trans. Inf. Theory **55**, 4337 (2009).

8. В. Ф. Бабкин, Проблемы передачи информации **7**, 13 (1971).

9. T. M. Cover and J. A. Thomas, *Elements of Information Theory*, Wiley (1991).

10. Р. Галлагер, *Теория информации и надежная связь*, Советское радио, Москва (1974).

11. Iwo Bialynicki-Birula, Phys. Rev. Lett. **80**, 5247 (1998).

12. В. А. Котельников, *О пропускной способности «эфира» и проволоки в электросвязи*, Всесоюзный энергетический комитет, *Материалы к I Всесоюзному съезду по вопросам технической реконструкции дела связи и развития слаботочной промышленности*, Изд. Управления связи Рабоче-крестьянской Красной армии (1933).

13. H. J. Landau and H. O. Pollak, Bell Syst. Techn. J. **40**, 65 (1961).

14. D. Slepian and H. O. Pollak, Bell Syst. Techn. J. **40**, 43 (1961).

15. W. H. J. Fuchs, J. Math. Anal. Appl. **9**, 317 (1964).

16. Л. Д. Ландау, Е. М. Лифшиц, *Статистическая физика*, т. V, часть I, Наука, Москва (1995).

17. C. E. Shannon, Bell Syst. Techn. J. **XXVII**, 379 (1948).

18. Yicheng Shi, Brenda Chng, and Ch. Kurtsiefer, Appl. Phys. Lett. **109**, 041101 (2016).