Письма в ЖЭТФ, том 119, вып. 7, с. 533 – 544

Реализация квантового генератора случайных чисел: экстракция доказуемо случайных битовых последовательностей из коррелированных марковских цепочек

К. А. Балыгин[+*], *С. П. Кулик*[*], *С. Н. Молотков*[×°]

[+]*Национальный исследовательский центр "Курчатовский институт", 123182 Москва, Россия*

[*]*Центр квантовых технологий, МГУ имени М. В. Ломоносова, 119899 Москва, Россия*

[×]*Академия криптографии Российской Федерации, 119331 Москва, Россия*

[°]*Институт физики твердого тела имени Ю. А. Осипьяна РАН, 142432 Черноголовка, Россия*

Поступила в редакцию 4 марта 2024 г.
После переработки 5 марта 2024 г.
Принята к публикации 5 марта 2024 г.

Представлена экспериментальная реализация квантового генератора случайных чисел. Впервые экспериментально реализован новый метод экстракции *доказуемо случайных битовых последовательностей* из коррелированных последовательностей фотоотсчетов – марковских цепей. *Достигнута скорость генерации 0 и 1 в* 154.5 *Мбит/с.* Обсуждаются также фундаментальные ограничения Природы на достижение истинной – идеальной случайности.

DOI: 10.31857/S1234567824070115, EDN: CHMAKN

Введение. В криптографических системах используются случайные числа, которые получаются как результат работы *физического генератора случайных чисел*, который является неотъемлемой частью системы и качество которого в значительной степени определяет стойкость системы.

Истинная случайность существует только в квантовой области, в том смысле, что результат измерения над квантовой системой каждый раз приготовленной в одних и тех же начальных условиях является принципиально непредсказуемым [1, 2].

Реализация физического генератора случайных чисел включает следующие стадии:

1. Выбор физической системы, измерения над которой дают первичную случайную последовательность.

2. Экстракция случайной битовой последовательности 0 и 1 из первичной последовательности.

Методы экстракции случайных последовательностей 0 и 1 из результатов измерений можно разделить на два класса: 1) вероятностные экстракторы, например, [3, 4]; 2) детерминистические экстракторы [2, 5–14].

Подходящим источником квантовой случайности, с точки зрения экспериментальной реализации, является акт поглощения фотонов – фотоотсчеты. Поскольку строго однофотонный источник отсутствует на сегодняшний день, то приходится использовать квазиоднофотонные состояния света – сильно ослабленное когерентное излучение лазера.

Если можно было бы обеспечить независимость последовательных во времени фотоотсчетов, то можно было бы использовать эффективные способы экстракции доказуемо истинно случайных последовательностей 0 и 1 [2]. Под истинно случайными последовательностями понимаются такие последовательности 0 и 1, в которых 0 и 1 независимы в каждой позиции, и вероятность $P(0) = P(1) = \frac{1}{2}$. *Однако существуют фундаментальные ограничения на скорость спадания корреляций между последовательными во времени измерениями. Любой случайный физический процесс, квантовый или классический, имеет спектр на положительной полуоси частот. В этом случае степень спадания корреляций случайной величины в разнесенные моменты времени, строго говоря, не может быть даже строго экспоненциальной, что диктуется фундаментальной теоремой Винера–Пэли [15]*[1)].

[1)]Заметим также, что теорема Винера–Пэли [15] приводит еще к одному фундаментальному последствию, а именно, процесс спонтанного распада (например, α-распад) не может быть экспоненциальным по времени – отклоняется от экспоненциального закона на малых и больших временах (см., например, детали в [16]). Отклонение от экспоненциального закона приводит к тому, что статистика отсчетов любого физического процесса *принципиально не может быть строго пуассоновской*. Процессы α-распада многие годы назад использовались для генерации случайных чисел, хотя не получили широкого применения из-за малой скорости и технического неудобства

Это означает, что извлекаемые из случайного процесса в разные моменты времени результаты измерений, строго говоря, оказываются коррелированными (зависимыми). Формально независимыми измерения становятся только при разнесении моментов измерения во времени на бесконечный интервал.

Физический сигнал – результат измерений $x(t)$ имеет спектр на положительной полуоси частот ω, т.е. $\omega \in [0, \infty)$, что приводит к фундаментальным ограничениям на скорость спадания корреляционной функции $\mathcal{K}(\tau) = \overline{x(t)x(t+\tau)}$ от времени. Согласно [15], для любой квадратично интегрируемой функции по времени (фактически имеющий конечную энергию), следующий интеграл должен сходиться (быть меньше бесконечности)

$$\int_{-\infty}^{\infty} \frac{|\log(\mathcal{K}(\tau))|}{1+\tau^2} d\tau < \infty.$$

Экспоненциальное спадание $\mathcal{K}(\tau) \propto e^{-\tau}$ приводило бы к логарифмической расходимости интеграла. Поскольку упомянутые ограничения на независимость измерений в последовательные моменты времени являются фундаментальным запретом Природы, то их принципиально невозможно обойти. *Максимум на что можно рассчитывать, так это на уменьшение корреляций между последовательными измерениями до желаемого уровня путем увеличения интервала времени T между измерениями. Формально лишь при $T \to \infty$ измерения становятся независимыми.*

Каждый текущий акт фотоотсчета зависит от последовательности отсчетов на предыдущих тактах. В эксперименте невозможно считать, что "глубина" предыстории является бесконечной, но естественно выбрать ее такой, чтобы зависимость от предыстории невозможно было заметить за время работы квантового генератора случайных чисел.

Таким образом, принципиально невозможно экспериментально "дотянуться" до идеальной случайности за конечное время.

Однако даже, в приближении конечной глубины корреляций между измерениями, крайне сложно доказать, что экстрагируется истинно случайная последовательность 0 и 1.

Для дальнейшего изложения, имеет смысл кратко, обсудить методы экстракции случайности. Вкратце первый метод на базе вероятностных экстракторов основан на следующих предположениях. Пусть имеется распределение вероятностей $P(x_1, x_2, \dots x_n)$ исходов измерений $(x_1, x_2, \dots x_n)$. Далее из некоторых модельных предположений оценивается величина, так называемой, min-энтропии – $H_{\min} = -\max_{(x_1,x_2,\dots x_n)} \log(P(x_1, x_2, \dots x_n))$. Пусть оценки min-энтропии дают $H_{\min} \geq k$, тогда теоретически можно получить не более k близких к случайным бит 0 и 1. Для экстракции случайных 0 и 1 из первичной последовательности измерений $(x_1, x_2, \dots x_n)$ используется сжатие – хэширование первичной последовательности при помощи хэш-функций – экстракторов. Более формально сжатие является отображением исходной последовательности длины n $\{0,1\}^n$ в последовательность меньшей длины $\{0,1\}^\ell$ $(\ell < n)$. При этом сама хэш-функция является случайной величиной. Иначе говоря, случайный выбор хэш-функции из некоторого множества функций требует *дополнительной случайности – битовой строки 0 и 1.* После сжатия получается не истинно случайная строка 0 и 1, а битовая строка ε с распределением $P(x)$ $(x \in \{0,1\}^\ell)$, *близкая к истинно случайной* с распределением $P_U(x) = \frac{1}{2^\ell}$

$$\sum_{x \in \{0,1\}^\ell} |P(x) - \frac{1}{2^\ell}| < \varepsilon.$$

Главная проблема в данном подходе состоит в том, что *оценка min-энтропии требует трудно контролируемых предположений о свойствах первичной последовательности результатов физических измерений.* Аккуратно можно оценить min-энтропию только для независимых результатов измерений, т.е. когда функция распределения распадается на произведение $P(x_1, x_2, \dots x_n) = P(x_1)P(x_2)\dots P(x_n)$. Второй важный момент состоит в том, что *случайный выбор хэш-функции требует дополнительной случайности.*

Возникает замкнутый круг – для экстракции случайности нужна дополнительная случайность.

Было предложено многократное использование случайности при выборе хэш- функции [3, 4]. Однако повторное использование случайности при выборе хэш-функции приводит к тому, что выходная последовательность 0 и 1 начинает все больше отклоняться от равновероятного распределения $P_U(x)$.

Детерминистические экстракторы не требуют дополнительной случайности.

реализации. По этой причине использование таких физических процессов для создания генераторов случайных чисел требует особой осторожности. Кроме того, в работе [17] было показано, что теорема Винера–Пэли вместе с принципом тождественности частиц приводит к фундаментальному пределу *скорости* генерации истинно случайных последовательностей 0 и 1. В квантовой области спектр гамильтониана устойчивой системы ограничен снизу, что, кстати, приводит к тому, что не существует эрмитового оператора времени в квантовой механики (время является параметром).

Поскольку при описании невозможно учесть зависимость текущего фотоотсчета от предыстории на бесконечное предыдущее время, то приходится ограничивать "глубину" – предысторию корреляций конечной величиной. Поэтому будем считать, что текущий фотоотсчет зависит от предыдущих исходов измерений на некоторую глубину. Данный параметр является свободным, и все выводы останутся справедливыми при любой конечной глубине корреляций. Адекватной моделью является марковская цепь случайных событий – последовательность фотоотсчетов или их отсутствие – $\{*, \sqcup\}$ в каждом такте. Вероятность события в каждом такте $*$ или $\sqcup$ зависит от предыдущих тактов на глубину r (r выбирается свободным.)

Ранее было показано [18], что в предположении конечной глубины корреляций, метод, используемый ниже, выдает на выходе действительно *истинно случайную последовательность 0 и 1 – любая позиция в выходной последовательности 0 и 1 реализуется строго с вероятностью $\frac{1}{2}$, и каждая позиция независима от остальных.* Данное принципиальное утверждение – доказуемая случайность имеет место при любой конечной глубине корреляций в марковской цепи. Истинная случайность – слишком "сильный и сложный" информационный ресурс, что даже в рамках приближений к реальной ситуации, доказательство истинной случайности является далеко нетривиальной задачей [14, 18].

Ниже, для самодостаточности изложения, приведем сначала метод экстракции доказуемо случайных последовательностей 0 и 1 из независимых последовательностей (см. детали в [2, 18]), затем применим метод экстракции доказуемо случайных последовательностей для марковских цепей (см. детали в [14,18]) в экспериментальной реализации квантового генератора случайных чисел.

Экстракция случайных битовых последовательностей из бернуллиевских последовательностей. Общая идея доказательства экстракции доказуемо случайных 0 и 1 из марковской цепи сводится к разбиению марковской цепи на классы эквивалентности одинаково вероятных последовательностей, к которым применяется метод нумерации Бабкина [19]. Подробные доказательства приведены в работе [18], ниже мы лишь упомянем необходимые моменты. Начнем с независимых бернуллиевских последовательностей. *Экспериментальная реализация квантового генератора случайных чисел, в предположении независимых измерений в первичных последовательностях, была сделана ранее [20–23].*

Пусть имеется источник независимых фотоотсчетов – бернуллиевская последовательность испытаний. *Экстракция истинно случайных последовательностей 0 и 1 из независимых бернуллиевских последовательностей происходит в два этапа.*

1) Первый этап: нумерация "на ходу" по мере возникновения бернуллиевской последовательности – присвоение номера по методу Бабкина [19] в классе эквивалентности последовательностей, имеющих одинаковую вероятность.

2) Второй этап: по номеру последовательности формируется блок *истинно случайных 0 и 1, последовательные блоки конкатинируются в выходную случайную последовательность.*

Пусть имеется источник, который порождает первичную последовательность – *символы* из *бинарного* алфавита $A = \{*, \sqcup\}$. Рассмотрим блок длиной n, где имеется k символов $*$. Всего таких блоков C_n^k. Пусть k символов $*$ встретились на местах $(i_1, i_2, \ldots.., i_k)$, $1 \le i_1 < i_2 < \ldots\ldots < i_k \le n$. Присвоим блоку номер

$$\mathrm{Num}(i_1, i_2, \ldots.., i_k) = \\ = C_{i_1-1}^1 + C_{i_2-1}^2 + \ldots\ldots C_{i_{k-1}-1}^{k-1} + C_{i_k-1}^k,$$

где полагается $C_j^i = 0$, если $j < i$. *Данное равенство дает метод нумерации В.Ф. Бабкина [19], который является "жемчужиной" арифметического кодирования без потерь.*

Извлечение блока $\{\varepsilon\}$ случайных 0 и 1 происходит из двоичного представления $(\varepsilon_{r_m+1}, \varepsilon_{r_m}, \varepsilon_{r_m-1}, \ldots, \varepsilon_1, \varepsilon_0)$ номера $\mathrm{Num}(i_1, i_2, \ldots i_k)$, и производится *по-разному*, в зависимости от того, в каком *диапазоне* чисел между 0 и $C_n^k - 1$ лежит номер $\mathrm{Num}(i_1, i_2, \ldots i_k)$ текущего блока. А именно:

номер	блок $\{\varepsilon\}$ случайных 0 и 1
$0 \le \mathrm{Num}(i_1, i_2, \ldots i_k) \le 2^{r_0} - 1$	$\varepsilon_{r_0-1}, \ldots, \varepsilon_0$
$2^{r_0} \le \mathrm{Num}(i_1, i_2, \ldots i_k) \le 2^{r_0} + 2^{r_1} - 1$	$\varepsilon_{r_1-1}, \ldots, \varepsilon_0$
$2^{r_0} + 2^{r_1} \le \mathrm{Num}(i_1, i_2, \ldots i_k) \le 2^{r_0} + 2^{r_1} + 2^{r_2} - 1$	$\varepsilon_{r_2-1}, \ldots, \varepsilon_0$
...	...
$2^{r_0} + \ldots + 2^{r_m} \le \mathrm{Num}(i_1, i_2, \ldots i_k) \le 2^{r_0} + \ldots + 2^{r_m} - 1$	$\varepsilon_{r_m-1}, \ldots, \varepsilon_0$

.

Пронумеруем строки (неравенства) номерами $0, \ldots, j, \ldots, m$. В j строке – *подклассе* – содержится 2^{r_j} различных номеров $\mathrm{Num}(i_1, i_2, \ldots i_k)$, которым *однозначно* соответствуют двоичные векторы из пространства $\{0,1\}^{r_j}$. Тогда, по каждому текущему номеру $\mathrm{Num}(i_1, i_2, \ldots i_k)$ на выход выдается соответствующий ему блок $\{\varepsilon\}$, состоящий из 0 и 1.

Цепь Маркова. Ниже кратко для самодостаточности изложения приведем необходимые сведения о цепях Маркова, поскольку полные доказательства являются довольно объемными (см. полные доказательства и детали в [18]).

В реальной ситуации имеется зависимость текущего состояния ($*$ – фотоотсчет, $\sqcup$ – отсутствие фотоотсчета в текущем такте) от предыдущих состояний. Будем считать, что такая зависимость распространяется на глубину r – предыдущих тактов измерений. Данная ситуация описывается цепью Маркова – текущее событие зависит от предыдущих, что задается переходной (условной) вероятностью. Наша цель – эффективно сгенерировать *случайные биты* из *простой однородной* цепи Маркова с *неизвестными* переходными вероятностями. Входная последовательность – цепь Маркова

$$X = x_1 x_2 ... x_N,$$

$x_i \in \{s_1, s_2, ..., s_n\}$ – состояния цепи, здесь n обозначает количество состояний цепи Маркова.

Сведение цепи Маркова с глубиной r к цепи с глубиной $r = 1$. Рассматриваемые ниже алгоритмы извлечения случайных бит справедливы для *простых однородных* цепей Маркова, т.е. *стационарных* (с *неменяющейся* матрицей переходных вероятностей) и имеющих порядок $r = 1$, где матрица переходных вероятностей задается в виде $P(s_j \mid s_i)$, $s_i, s_j \in \{s_1, ..., s_n\}$, поэтому требуется свести цепь Маркова с глубиной $r > 1$ к простой цепи с $r = 1$. *Это делается путем увеличения размерности состояний цепи.* Вероятность произвольной последовательности символов $X_N = x_1 x_2 ... x_N$ определяется как

$$P(X_N) = P(x_1) \prod_{i=1}^{N-1} P(x_{i+1} \mid x_i).$$

На практике, при построении квантового генератора случайных чисел имеем *символы* из *бинарного* алфавита $A = \{*, \sqcup\} = \{0,1\}$ и некоторый произвольный порядок $r > 1$. В этом случае цепь Маркова задается начальным распределением $P(\epsilon_1, ..., \epsilon_r)$ с матрицей переходных вероятностей $P(\epsilon_{r+1} \mid \epsilon_1, ..., \epsilon_r)$, $\epsilon_i \in \{0,1\}$. Вероятность траектории – первичной последовательности, есть

$$X_N = \varepsilon_1 \varepsilon_2 ... \varepsilon_N, \varepsilon_i \in \{0,1\}$$

$$P(X_N) = P(\varepsilon_1, ..., \varepsilon_r) \prod_{i=1}^{N-r} P(\varepsilon_{i+r} \mid \varepsilon_i, ..., \varepsilon_{i+r-1}).$$

Перейти к *простой* цепи Маркова с глубиной $r = 1$ можно путем укрупнения алфавита. Введем новый алфавит $A' = \{s_1, ..., s_n\} = 0...0, \ldots, 1...1 = 2^r$, объединяя соседние r символов в траектории $X_N = \varepsilon_1 \varepsilon_2 ... \varepsilon_N$ с зацеплением на 1 позицию в один символ. Тогда новые символы $X_{N-r} = x_1 x_2 ... x_{N-r}$ *будут зависеть только от одного своего предшественника*, имеем

$$P(\varepsilon_{i+r} \mid \varepsilon_i, ..., \varepsilon_{i+r-1}) = \\ = P(\varepsilon_{i+1}, ..., \varepsilon_{i+r-1}\varepsilon_{i+r} \mid \varepsilon_i, ..., \varepsilon_{i+r-1}) = \\ = P(x_{i+1} \mid x_i).$$

Выходные последовательности из марковской цепи. Для построения метода экстракции случайных 0 и 1 необходимо ввести *разбиение на классы эквивалентности на множестве последовательностей с одинаковой вероятностью [2, 18].* Введем понятие выходных последовательностей [18], имеем

$$X_N = x_1 x_2 ... x_N, \tag{1}$$

$$\pi(X_N) = \{\pi_1(X_N), \pi_2(X_N), \ldots, \pi_M(X_N)\}, \\ \pi_i(X_N) = \{x_j : x_(j-1) = s_i\}, \tag{2}$$

т.е. это множество последовательностей $\pi_i(X_N)$-х, где выходной $\pi_i(X_N)$-й блок представляет собой подпоследовательность символов, следующих за s_i. Последовательность однозначно задается своим первым элементом и набором выходных последовательностей (блоков), иными словами, существует взаимно-однозначное отображение между X_N и парой $(x_1, \pi(X_N))$.

Иллюстративные примеры. 1) Приведем пример формирования выходных блоков $\pi(X_N)$ из марковской цепи с $r = 1$, для бинарного алфавита, пусть

$$X_N = x_1, \ldots, x_N = 01001011100010100011010001, \tag{3}$$

сформируем блок $\pi_i(X_N)$, отметим состояния, которые следует за 0 и за 1, получаем

$$\pi_0(X_N) \quad 0 \to = 101100110011001, \tag{4}$$

$$\pi_1(X_N) \quad 1 \to = 0011000101000. \tag{5}$$

Суммарное число бит $N - 1$, поскольку первый 0 никуда не входит.

2) Теперь, пусть марковская цепь с предысторией на глубину 2 шага, $r = 2$, имеем состояния цепи s_i $(i = 1, 2, 3, 4)$,

$$s_1 = 00, \quad s_2 = 01, \quad s_3 = 10, \quad s_4 = 11. \tag{6}$$

Укрупнение алфавита приводит к последовательности

$$01001011100010100011011000 1 = \tag{7}$$

$$= 01.10.00.01.10.01.11.11.10.00.00.01.10.01.10.00.00.01.11.10.01.11.10.00.00.01 =$$

$$= 2.3.1.2.3.2.4.4.3.1.1.2.3.2.3.1.1.2.4.3.2.4.3.1.1.2.$$

Последняя последовательность представляет собой простую однородную цепь Маркова, имеем

$$\pi_1(X_N) \quad 1 \to 2.1.2.1.2.1.2, \tag{8}$$

$$\pi_2(X_N) \quad 2 \to 3.3.4.3.3.4.4, \tag{9}$$

$$\pi_3(X_N) \quad 3 \to 1.2.1.2.1.2.1, \tag{10}$$

$$\pi_4(X_N) \quad 4 \to 4.3.3.3. \tag{11}$$

Принципиальный вопрос сводится к следующему. Какие перестановки в блоках $\pi_i(X_N)$ допустимы? Какие перестановки отвечают существующим цепям Маркова и сохраняют вероятность переставленной последовательности. Было показано [14, 18], что, если имеются две марковские цепи X_N и X'_N, которые начинаются с одинакового элемента s_1 и заканчиваются элементом s_χ, то две марковские цепочки с $\pi(X_N)$ и $\pi'(X'_N)$ входят в один класс эквивалентности и имеют одинаковую вероятность, если имеет место

$$\pi(X_N) = \{\pi_1, \pi_2, ..., \pi_\chi ..., \pi_N\}, \quad \pi'(X'_N) = \{\Lambda_1, \Lambda_2, ., \Lambda_\chi .., \Lambda_N\}, \tag{12}$$

$$\pi_i \doteq \Lambda, \quad i \neq \chi \quad \text{перестановка с фиксированным последним элементом } \pi_i,$$

$$\pi_i \equiv \Lambda, \quad i = \chi, \quad \text{любые перестановки } \pi_i.$$

Обратно, если имеют место перестановки в $\pi(X_N)$, то существует марковская цепь с той же вероятностью. Данное свойство позволяет разбить все марковские цепочки на классы эквивалентности одинаково вероятных последовательностей. Далее из классов эквивалентности происходит экстракция случайных последовательностей 0 и 1.

Экстракция "на ходу". В этом разделе приведем метод экстракции случайных 0 и 1 "на ходу" (см. детали в [18]).

Входные данные:

Последовательность $X = x_1 x_2 ... x_N$ – цепь Маркова, где $x_i \in S = s_1, s_2, ..., s_n$.

Параметры:

Размер окна ϖ. Окно необходимо, чтобы вырезать последовательные блоки из $\pi_i(X)$ размером ϖ. Ширина окна ϖ выбирается при реализации.

Выход алгоритма:

Последовательность или поток истинно случайных 0 и 1.

Данный алгоритм *распараллеливает* поступающие состояния траектории цепи Маркова на выходные последовательности $\pi_1(X), ..., \pi_n(X)$, добавляя следующий s_j в последовательность $\pi_i(X)$, *только* если перед s_j было состояние s_i.

Пусть в последовательности $\pi_i(X)$ *набрался* текущий блок F_{ik}, $k = 1, 2, ...$, размера ϖ, тогда он:

∘ *сразу* отправляется для *преобразования в биты – 0 и 1*, если последний элемент в F_{ik} *как раз* равен s_i;

∘ если последний элемент в F_{ik} не равен s_i, то блок F_{ik} *ждет отправки* на обработку до тех пор, пока в цепи Маркова не появится s_i;

∘ блок F_{ik} *вообще не отправляется* на обработку, если ему не удалось дождаться появления s_i.

В этом смысле мы можем говорить, что *наполненные* блоки в *параллельных* выходных последовательностях $\pi_1(X), ..., \pi_n(X)$ *становятся в очередь* на обработку. Их *считывание* данным алгоритмом *не совпадает с естественно-временным* появлением блоков.

Как было показано в [18], такой порядок считывания блоков, какой задается алгоритмом для данной траектории цепи Маркова, *сохраняется также и при считывании блоков любой* траектории цепи Маркова в классе *эквивалентности* S, что открывает *прямой путь к равновероятноти выходной двоичной последовательности на выходе алгоритма Бабкина по аналогии с независимым источником.*

Приведем пример. Пусть $N = 29$, $n = 2$, $\varpi = 3$.

$$X = s_1s_2s_2s_1s_1s_2s_2s_1s_1s_2s_2s_1s_1\mathbf{s}_2s_2s_1s_1\mathbf{s}_2s_2s_1s_1s_2s_2s_1s_1s_2s_2s_1s_1$$

$$\pi_1(X) = E_1 = \overbrace{s_2--s_1s_2}^{F_{11}} - \overbrace{s_1s_2--s_1}^{F_{12}}\overbrace{s_2--s_1s_2}^{F_{13}} - \overbrace{s_1s_2--s_1}^{F_{14}}\overbrace{s_2--s_1}^{E_1},$$

$$\pi_2(X) = E_2 = -\overbrace{s_2s_1--s_2}^{F_{21}}\overbrace{s_1--s_2s_1}^{F_{22}} - \overbrace{s_2s_1--s_2}^{F_{23}}\overbrace{s_1--s_2s_1}^{F_{24}} - \overbrace{s_2s_1}^{E_2}-.$$

Порядок считывания блоков *алгоритмом*

$$F_{21}.....F_{11}.....F_{12}.....F_{22}.....F_{23}.....F_{13}.....F_{14}.....F_{24}.$$

Естественно-временной порядок считывания блоков

$$F_{11}.....F_{21}.....F_{22}.....F_{12}.....F_{13}.....F_{23}.....F_{24}.....F_{14}.$$

Как было доказано в [18], алгоритм выдает истинно случайную последовательность 0 и 1 "на ходу" из марковской цепи.

Разобьем все возможные последовательности из ${s_1, s_2, ..., s_n}^N$ на классы *эквивалентности, имеющих одинаковую вероятность*. Рассмотрим последовательность X и включим X' в класс S, если:

1) $x_1 = x'_1$ и $x_N = x'_N$ – *начало и конец совпадают,*

2) для всех $1 \le i \le n$

$$\pi_i(X) = F_{i1}F_{i2}...F_{im_i}E_i, \tag{13}$$
$$\pi_i(X') = F'_{i1}F'_{i2}...F'_{im_i}E_i,$$

где F_{ij} и F'_{ij} — блоки, используемые для генерации выходных данных,

3) для всех i, j имеем $F_{ij} \equiv F'_{ij}$ – *полная перестановка.*

Не обрабатываемые части E_i для последовательностей X и X' совпадают. Кроме этого, как следует из разделов выше, последовательности в классе S *имеют одинаковую вероятность.*

В выходных последовательностях $\pi_i(X) = F_{i1}F_{i2}...F_{im_i}E_i$, $1 \le i \le n$, последовательность блоков $F_{i1}, F_{i2}, ...F_{im_i}$ определяет порядок, в котором эти блоки отправляются на обработку по алгоритму Бабкина для экстракции случайных 0 и 1. В то же время, *глобальный* порядок следования блоков

$$F_{11}, F_{i2}, ...F_{1m_1}, F_{21}, F_{22}, ...F_{2m_2}, ..., F_{n1}, F_{n2}, ...F_{nm_n} \tag{14}$$

в *реальном* времени появления состояний цепи Маркова может быть весьма *произвольным, но строго задаваемым* исходной цепью Маркова $X = x_1x_2...x_N$.

Глобальный порядок следования блоков для всех траекторий $X' = x'_1x'_2...x'_N$ из класса S сохраняется и равен

$$F'_{11}, F'_{12}, ...F'_{1m_1}, F'_{21}, F'_{22}, ...F'_{2m_2}, ..., F'_{n1}, F'_{n2}, ...F'_{nm_n}.$$

Далее, как и в случае *независимого* источника, блоки F_{ij} по мере появления обрабатываются алгоритмом Бабкина. Выход из каждого блока $\Psi(F_{ij})$ есть блок истинно случайных 0 и 1. Данные блоки последовательно конкатенируются – последовательно соединяются, в данном примере, имеем

$$\Psi(F_{11}) \parallel ... \parallel \Psi(F_{nm_n}) = Y_{11} \parallel ... \parallel Y_{nm_n} = Y.$$

Как было показано в [18], с использованием *одинаковой вероятности* траекторий цепи Маркова в классах *эквивалентности, что выходные последовательности при любой длине ℓ содержат всевозможные комбинации 0 и 1*

$$\overbrace{(000...000)}^{\ell},\overbrace{(000...001)}^{\ell},...,\overbrace{(111...111)}^{\ell},$$

и все такие последовательности имеют одинаковую вероятность $2^{-\ell}$*, независимо от глубины корреляций. В этом случае отдельные биты, как случайные величины, являются независимыми и равновероятными, т.е. являются истинно случайными.*

Экспериментальная реализация квантового генератора случайных чисел. При реализации требуется совместить два взаимно противоречивых требования. 1) Для достижения большой скорости генерации случайных чисел требуется увеличивать тактовую частоту, что приводит к корреляциям между последовательными результатами измерений из-за того, что детектор не готов к регистрации в следующем такте – имеет "мертвое" время. 2) Для достижения однофотонного режима (точнее квазиоднофотонного) требуется уменьшать интенсивность излучения – среднее число фотонов в каждом такте, что приводит к снижению темпа фотоотсчетов, и, соответственно, скорости генерации случайных чисел.

Вторая проблема решается использованием не отдельного детектора, а матрицы детекторов – SIPM матрицы (Silicon Photo Multiplier), содержащей большое число детекторов. При этом вероятность регистрации фотонов пропорциональна числу пикселей в SiPM, что позволяет снизить среднее число фотонов. Первая проблема также решается, вероятность того, что фотон попадет в детектор, который сработал на предыдущем также, и еще не готов к регистрации, обратно пропорциональная числу пикселей.

Таким образом, использование матрицы SiPM решает упомянутые проблемы. Функциональная схема генератора представлена на рис. 1.

В качестве детектора был выбран сенсор SiPM (EQR15-22-1313D-S, Китай), имеющий 4 отдельных матрицы SiPM в одном корпусе. Площадь отдельного элемента составляла $S_p = 1.3 \times 1.3\,\text{мм}^2$, с числом пикселей $N_p = 4444\,1/\text{мм}^2$. Квантовая эффективность η отдельного детектора составляла $\eta \approx 15\,\%$ на длине волны 0.635 мкм. Характерный темп темновых отсчетов матрицы SiPM 250 КГц. Источником излучения являлся светодиод с рабочей длиной волны излучения $\lambda = 635$ мкм. Для обработки использовалась (ПЛИС) FPGA фирмы MAX 10 (Intel). Частота набора первичной последовательности составляла 180 МГц. Внешний интерфейс для выдачи результирующей случайной последовательности в непрерывном потоке – USB 2.0.

Достигнутая скорость генерации случайных 0 и 1 составила 154.5 *Мбит/с.*

Среднее число фотонов, приходящихся на пиксел. Оценим среднее число фотонов, падающих на отдельный пиксел. Эта оценка важна для того, чтобы быть уверенным, что генератор работает как квантовый, и, действительно, регистрируются фотоотсчеты от квазиоднофотонного излучения. Была оценена вероятность отсчета за один такт на SiPM $P(*) \approx 0.45$, отсюда среднее число фотонов на один пиксел $\mu = P(*)(\eta N_p/S_p) = 0.52/(0.15 \cdot 4444/1.3 \cdot 1.3) \approx 1.3 \cdot 10^{-3}$. Таким образом, реализован практически однофотонный режим.

Распределение интервалов, корреляционная функция. Если бы результаты измерений в тактах были бы независимыми, то мы бы имели дело с бернуллиевской последовательностью с вероятностями фотоотсчета $P(*)$ и вероятностью отсутствия $P(\sqcup) = 1 - P(*)$. Функция распределения временных интервалов между соседними фотоотсчетами $*$, разделенными k тактами (Time Slots), есть *геометрическое распределение* $P_{\text{Bern}}(T) = (1 - P(*))^{T-1}P(*)$. Напомним, что интервал T принимает дискретные значения $T = n\tau$ ($\tau = 1/180$ Мгц, n – число тактов). Логарифм функции распределения $\log(P_{\text{Bern}}(T))$ представляет собой прямую. Пусть $P_{\text{Exp}}(T)$ – реальная экспериментальная функция распределеия интервалов, соответственно, $\log(P_{\text{Exp}}(T))$. Если сдалать "подгонку" экспериментальной зависимости $\log(P_{\text{Exp}}(k))$ прямой $\log(P^{\text{Fit}}_{\text{Bern}}(T))$, то разность $\Delta(T) = \log(P^{\text{Fit}}_{\text{Bern}}(T)) - \log(P_{\text{Exp}}(T))$ будет давать наглядную меру отклонения экпериментального распределения от независимой бернуллиевской последовательности. Зависимость $\Delta(T)$ приведена на рис. 2, откуда видно, что существуют зависимость между отсчетами. Видно также, что существенные корреляции (предыстория между отсчетами) распространяется примерно на глубину 10 тактов. Именно, такая глубина марковской цепи выбрана для реализации алгоритма экстракции. Выбор более мощной FPGA позволяет учесть большую глубину корреляций марковской цепи. Как будет видно ниже, при проведении тестов на случайность, глубина $r = 10$ оказывается достаточной. Еще одной характеристикой глубины марковской цепи является *корреляционная функция первичной последовательности измерений*, которая была определена как среднее по выборке $\text{CorrFun}(T = n\tau) = \frac{\sum_i^N s(i)}{N}$, где $N = 8 \cdot 10^9$ бит – длина выборки, $s(n) = -1$, если $x(i) \oplus x(i + n) = 0$, и $s(n) = 1$, если $x(i) \oplus x(i + n) = 1$. Зависимости $\text{CorrFun}(T = n\tau)$ приведены на рис. 3. Для независимой бернуллиевской последовательности $\text{CorrFun}(T = n\tau)$ должна быть прямой горизонтальной линией, не зависящей от T. Как видно из

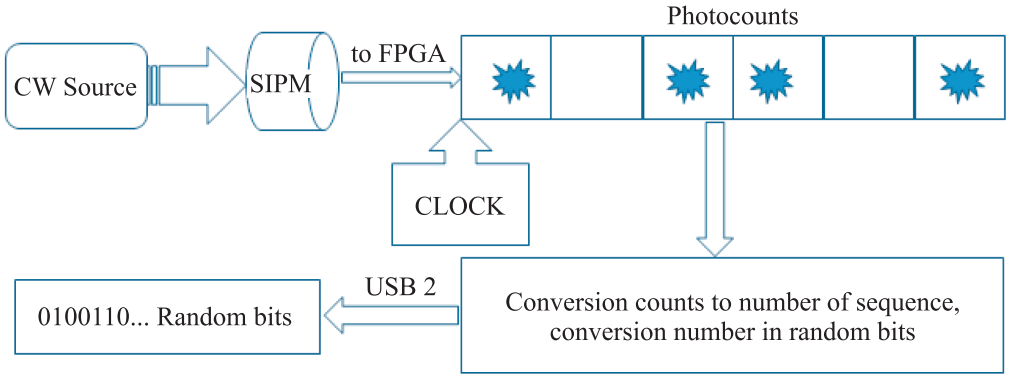

Рис. 1. (Цветной онлайн) Функциональная схема генератора случайных чисел

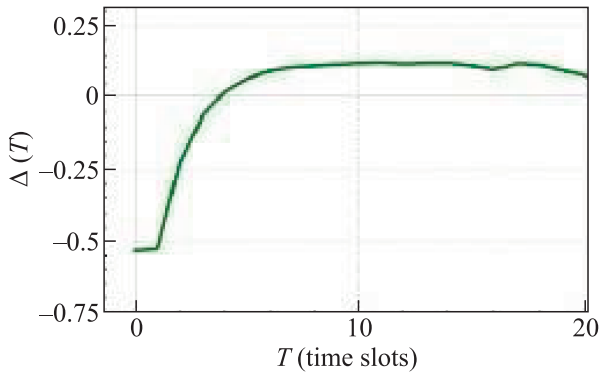

Рис. 2. (Цветной онлайн) Зависимость уклонения логарифма экспериментального распределения от логарифма геометрического распределения как функция числа тактов

рис. 3, глубина корреляций составляет не более 10 тактов, что оправдывает выбор глубины марковской цепи $r = 10$.

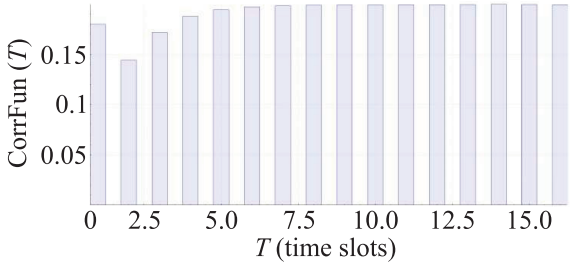

Рис. 3. (Цветной онлайн) Корреляционная функция в зависимости от числа тактов между измерениями

Статистические тесты случайных последовательностей. Для проверки однородности по числу 0 и 1 в выходной случайной последовательности был проведен отдельный тест на большой выборке, а именно, было сгенерировано 100 последовательностей, каждая длиной $8 \cdot 10^9$ бит, для каждой последовательности вычислялась разница 0 и 1. График зависимости разницы $(\delta_{0/1}(n))$ как функция номера серии n, приведен на рис. 4 как функция числа последовательностей. Средняя разница по 0 и 1 по всем сериям составила $9.2 \cdot 10^{-8}$, что с запасом укладывается в интервал 3-сигма $(\frac{3}{2}\sqrt{\frac{1}{100 \cdot 8 \cdot 10^9}} = 1.7 \cdot 10^{-6})$.

В открытой печати имеется несколько наборов тестов на случайность [24]. Для проверки статистических свойств случайных последовательностей нами был выбран стандартный набор тестов NIST [24]. Данный набор тестов является минимально необходимым и является основанием для исследования последовательностей другими наборами специальных тестов. Кратко остановимся на идеологии проверки последовательности на случайность.

Как уже упоминалось выше, нельзя доказать, что данная последовательность произошла из источника истинной случайности, можно лишь утверждать, что она не противоречит гипотезе случайности по некоторому статистическому критерию.

Проверяется гипотеза H_0 о том, что последовательность является истинно случайной. При этом предположении, различные статистики S – группировки 0 и 1 также являются случайными величинами, распределения вероятностей различных статистик при длине последовательности $n \to \infty$ должны стремиться к некоторым эталонным распределениям для случайной последовательности. Фиксируется некоторый уровень значимости α и пороговое значение для каждой статистики. Если вероятность уклонения статистики превышает пороговое значение, то гипотеза о случайности отклоняется. Это означает лишь то, что даже генератор идеальных случайных последовательностей может выдать последовательность, которая имеет такое уклонение.

Далее, подсчитывается вероятность *P-value* – вероятность того, что даже идеальный случайный ис-

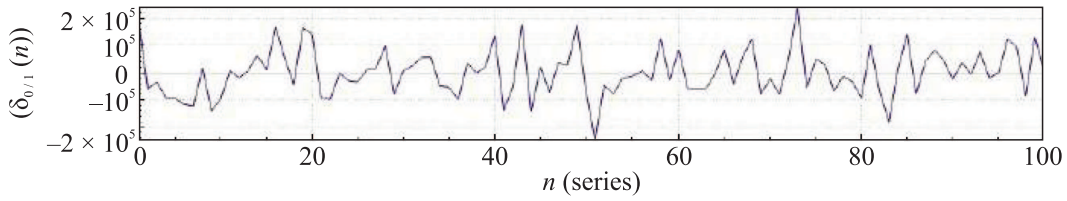

Рис. 4. (Цветной онлайн) Разность 0 и 1 как функция номера серии, каждая длиной $8 \cdot 10^9$ бит

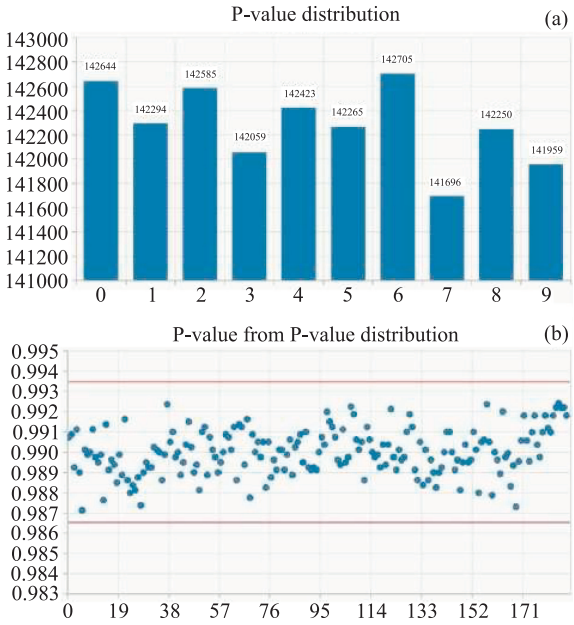

Рис. 5. (Цветной онлайн) (a) – Зависимости числа последовательностей по всем тестам, для которых значения $P - value$ попадают в один из 10 интервалов. (b) – График *P-vaue* от *P-value*. По горизонтали показаны номера тестов от 1 до 16 по 10 сериям

точник может выдать последовательность с таким уклонением статистики. Если $P > \alpha$, то гипотеза H_0 принимается, при $P < \alpha$, гипотеза отклоняется, последовательность считается не случайной.

P-values для различных тестов. Интерпретация *P-value*-значения. При заданном уровне значимости α, *P-value* имеется вероятность того, что даже идеальный генератор может сгенерировать с такой вероятностью последовательность, которая будет выглядеть как не случайная для данного теста. Чем меньше *P-value*, тем с меньшей вероятностью идеальный генератор "имеет право" сгенерировать такую последовательность. Если вычисленное *P-value* больше α, то тест считается пройденным. Стандартное значение уровня значимости для $\alpha \in [0.001, 0.01]$ [24]. Было использовано значение $\alpha = 0.01$.

Были проведены тесты с разными длинами и числом тестируемых последовательностей, полное число тестов составило 188. Число тестируемых последовательностей $M = 8000$, длина каждой последовательности равнялась $L = 1 \cdot 10^6$ бит. Для ряда тестов существует несколько проверок с различными шаблонами (см. детали в NIST [24]). Тест *Non Overlapping Template* был проведен для 148 шаблонов. Тест *Random Excursions* – для 8 вариантов. Тест *Random Excursions Variant* – для 18 вариантов параметров. Тест *Serial* – для двух вариантов параметров. Для данных тестов в табл. 1 указаны максимальное/минимальное значение доли последовательностей и значений *P-value*. Результаты тестов приведены в табл. 1.

Для одного теста – монобитный тест, кроме теста в стандартной идеологии NIST (см. табл. 1), был проведен для последовательности $100 \cdot 8 \cdot 10^9$ бит (см. выше рис. 4), в отличии от других тестов, требующих большой компьютерной памяти, данный тест можно провести "на ходу".

Доля последовательностей, прошедших тесты сама является случайной величиной. Допустимый диапазон флуктуаций определяется дисперсией *P-value*. *P-value* являются случайными величинами с распределением Бернулли с двумя исходами. Один исход – тест пройден, второй исход – тест не пройден, Допустимый разброс *P-value* должен укладываться в "три сигма". Величина дисперсии для *P-value* есть $\sqrt{\frac{P(1-P)}{M}}$ (M – число тестируемых последовательностей).

Согласно [24], при уровне значимости $\alpha = 0.01$ все *P-value* должны попадать в интервал "три сигма" $1 - P \pm 3\sqrt{\frac{P(1-P)}{M}} = 0.99 \pm 3\sqrt{\frac{0.99 \cdot 0.01}{M}}$.

Интервал "три сигма" оказывается равным $[0.987, 0.993]$ ($M = 8000$). Как видно из табл. 1 и рис. 5a доля последовательностей, прошедших тесты, укладывается в доверительный интервал "три сигма" с хорошим запасом. По данному критерию гипотеза о происхождении последовательностей из случайного источника является справедливой.

Однородность значений P-values. Напомним, что *P-value* само является случайной величиной. Поэтому частота появлений значений *P-values* для раз-

Таблица 1. Значения *P-value* и доля последовательностей, прошедших различные тесты

N	Название теста $M = 8000$ $L = 1 \cdot 10^6$	*P*-value	Доля последовательностей
1	Frequency Test	0.02415	0.99075
2	Block Frequency	0.89185	0.99087
3	Runs	0.56080	0.98925
4	Longest Runs	0.93061	0.99113
5	Rank	0.32405	0.98900
6	FFT Fast Fourier Transform	0.11899	0.9879
7	Non Overlapping Template	0.99519/0.02896	0.99238/0.98950
8	Overlapping Template	0.25798	0.98800
9	Cumulative Sums	0.14502	0.99000
10	Cumulative Sums Reverse	0.62619	0.98962
11	Universal	0.61423	0.99050
12	Approximate Entropy	0.00616	0.98787
13	Random Excursions	0.86223/0.18553	0.99201/0.86223
14	Random Excursions Variant	0.94519/0.04949	0.99242/0.98955
15	Serial	0.47163/0.09752	0.99238/0.99050
16	Linear Complexity	0.68127	0.99062

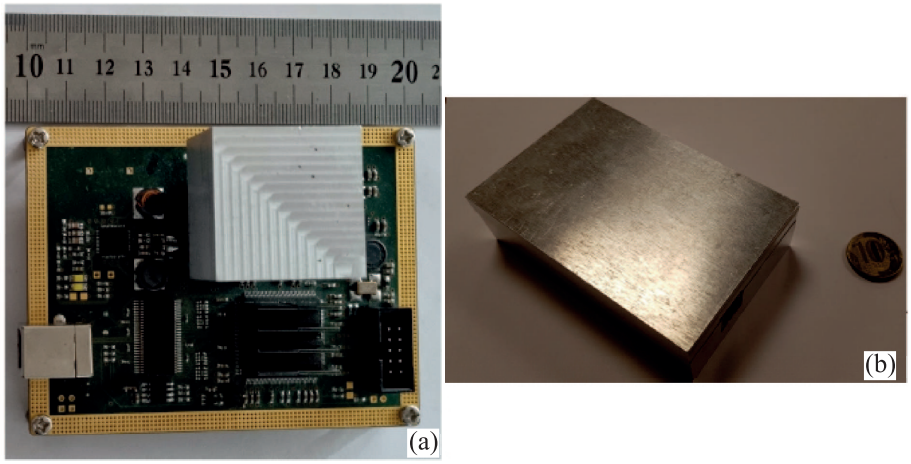

Рис. 6. (Цветной онлайн) (a) – Внешний вид генератора случайных чисел без внешнего корпуса – отладочный вариант. (b) – Внешний вид генератора в экранированном в корпусе

личных тестов при большом объеме выборки распределена по нормальному закону. Если величины распределены по нормальному закону, статистика, которая приводится ниже, имеет распределение Пирсона (см., например, [25]). Тест на однородность значений *P-value*. При большом числе тестируемых последовательностей суммарное значение *P-value* по всем тестам есть сумма одинаково распределенных случайных величин, которая распределена по гауссовскому нормальному закону [25]. Определим статистику $X_N^2 = \sum_{j=1}^{N} \frac{(\nu_j - N \cdot p_j)^2}{N \cdot p_j}$, где ν_j – доля значений *P-value*, попадающих в j-й интервал [0,1], p_j – истинная вероятность попадания в j-й интервал. При большом числе тестируемых последовательностей распределение вероятностей данной статистики X_N^2 не зависит от распределения p_j, входящих в нее величин, и стремится к распределению Пирсона $\chi^2(N-1)$ с $(N-1)$-й степенью свободы [25]. Рекомендуемое тестами NIST число интервалов равно $N = 10$ [24]. Пороговое значение при нулевой гипотезе (H_0 – последовательность случайна) допустимого разброса получается при заданном уровне значимости α из соотношения $\Pr\{X_N^2 > t_\alpha | \mathrm{H}_0\} = \alpha$, где $t_\alpha = \chi^2_{1-\alpha,N-1}$ – $(1-\alpha)$-я квантиль распределения χ^2 с $(N-1)$-й степенью свободы. В нашем случае $N = 10$ – число интервалов для значений *P-value*. Иными словами,

если уклонение статистики $X_N^2 > \chi^2_{1-\alpha,N-1}$, то нулевая гипотеза H_0 отвергается, последовательность считается не случайной, поскольку уклонение статистики от допустимой нормы (при заданной вероятности – уровне значимости) превышено. Тест на однородность *P-value* считается пройденным, если *P-value* от *P-value*

$$\hat{P} = \frac{\int_{X_K^2}^{\infty} dx e^{-x/2} x^{K/2-1}}{2^{K/2}\Gamma(K/2)}, \quad K = N-1,$$

не менее $\hat{P} > 0.0001$, то тест на однородность считается пройденным, и принимается H_0 гипотеза.

На рисунке 5b приведены результаты теста на равномерность *P-value*. Значение *P-values* от *P-value* – равно: *P-value* = 0.722. *P*-values от *P*-values должны быть больше критического $\hat{P}_c > 0.0001$. Тест на равномерность *P-value* с запасом пройден. Для всех тестов доля последовательностей, прошедших тесты по величинам *P-value* лежит в пределах "три сигма", что означает успешное прохождение тестов – гипотеза о случайности последовательности принимается.

Внешний вид генератора представлен на рис. 6.

Заключение. Для независимых измерений существуют эффективные методы экстракции истинно случайных последовательностей 0 и 1 из исходной последовательности [2, 18, 19].

Однако существуют фундаментальные ограничения Природы на скорость спадания корреляций между результатами измерений во времени, поэтому "дотянуться" до истинной случайности можно лишь за неограниченное время. Корреляции (зависимость) между измерениями *проникают* на неограниченную глубину по времени.

Эксперименты всегда проводятся на конечном временном отрезке, поэтому результаты последовательных измерений невозможно сделать независимыми. Все, что нам позволяется Природой, так это учитывать корреляции между измерениями на *конечную глубину* по времени. Причем явный (функциональный) вид корреляций в ситуации реального эксперимента неизвестен. Неизбежно приходится прибегать к приближениям. Адекватным приближением является учет корреляций на конечную глубину, которое дается стационарными цепями Маркова конечного порядка. В этом приближении корреляции описываются переходными (условными) вероятностями между результатами измерений. Важно, что явный вид самих переходных вероятностей неизвестен и не требуется при построении алгоритмов экстракции случайных битов.

В приближении конечной глубины корреляций удается получить доказуемо случайные выходные битовые последовательности даже при зависимых исходах измерений. В этом подходе, в отличие от других подходов, например, с вероятностными экстракторами, используется фактически единственное предположение – о конечной глубине корреляций. Любые подходы к получению истинной случайности, по причине фундаментальных ограничений Природы, являются лишь приближением. Вопрос состоит лишь в том, насколько конкретное приближение адекватно описывает реальную ситуацию и сколько предположений содержится внутри данного приближения.

Доказательство случайности выходной битовой последовательности является нетривиальной задачей даже в рамках выбранного приближения. Далеко не все подходы позволяют получить доказуемую случайность.

Авторы выражают благодарность И. М. Арбекову, А. Н. Климову, А. А. Калинкину, В. О. Миронкину, а также сотрудникам: СФБ Лаборатории В. А. Кирюхину, ИнфоТекс А. В. Уривскому за активное сотрудничество. Отдельная благодарность С. С. Негодяеву за помощь в реализации тестов NIST.

Финансирование работы. Работа выполнялась в рамках госзадания. Никаких дополнительных грантов на проведение или руководство данным конкретным исследованием получено не было.

Конфликт интересов. Конфликт интересов у авторов отсутствует.

1. M. Herrero-Collantes and J. Carlos Garcia-Escartin, Rev. Mod. Phys. **89**, 015004 (2017).
2. И. М. Арбеков, С. Н. Молотков, Успехи физических наук **191**, 651 (2021).
3. R. Shaltiel, Lect. Notes Comput. Sci. **6756**, 21 (2011).
4. A. De, Ch. Portmann, Th. Vidick, and R. Renner, arXiv:0912.5514 [quant-ph].
5. M. Blum, Combinatorica **6**, 97 (1986).
6. J. von Neumann, Appl. Math. Ser., Notes by G. E. Forstyle, Nat. Bur. Stand. **12**, 36 (1951).
7. W. Hoeffding and G. Simon, Ann. Math. Statist. **41**, 341 (1970).
8. Q. Stout and B. Warren, Ann. Probab. **12**, 212 (1984).
9. Y. Peres, Ann. Statist. **20**, 590 (1992).
10. P. Elias, Ann. Math. Statist. **43**, 865 (1972).
11. D. Knuth and A. Yao, *The complexity of nonuniform random number generation, Algorithms and Complexity: New Directions and Recent Results*, Academic Press, N.Y. (1976), p. 357.

12. T. S. Han and M. Hoshi, IEEE Trans. Inform. Theory **43**(2), 599 (1997).
13. P. A. Samuelsons, J. Amer. Statist. Assoc **63**(324), 1526 (1968).
14. H. Zhou and J. Bruck, IEEE Trans. Inform. Theory **58**, 2490 (2012).
15. Н. Винер, Р. Пэли, *Преобразование Фурье в комплексной области*, Наука, М. (1964), 268 с.
16. L. Fonda, G. C. Ghirardi, and A. Rimii, Rep. Prog. Phys. **41**, 587 (1978).
17. S. N. Molotkov, Laser Phys. Lett. **20**, 035202 (2023).
18. И. М. Арбеков, С. Н. Молотков, Успехи физических наук, в печати; DOI: 10.3367/UFNr.2024.02.039658.
19. В. Ф. Бабкин, Проблемы передачи информации **7**, 13 (1971).
20. С. Н. Молотков, Письма в ЖЭТФ **105**, 374 (2017).
21. К. А. Балыгин, В. И. Зайцев, А. Н. Климов, С. П. Кулик, С. Н. Молотков, ЖЭТФ **153**, 879 (2018).
22. K. A. Balygin, V. I. Zaitsev, A. N. Klimov, S. P. Kulik, S. N. Molotkov, E. Popova, and S. Vinogradov, Phys. Lett. **14**, 125207 (2017).
23. К. А. Балыгин, В. И. Зайцев, А. Н. Климов, С. П. Кулик, Письма в ЖЭТФ **106**, 451 (2017).
24. *A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications*, http://csrc.nist.gov/rng/SP800-22b.pdf.
25. Г. И. Ивченко, Ю. И. Медведев, *Введение в математическую статистику*, Издательство ЛКИ, М. (2010), 600 с.