# ГЕНЕРАЦИЯ КРИПТОГРАФИЧЕСКИ СТОЙКИХ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ПОМОЩЬЮ БЛЕНДЕРА

*Грозов В.А.[1], Будько М.Ю.[2], Гирик А.В.[3]*

***Ключевые слова:*** *защита данных, ГОСТ Р 34.12-2015 «Кузнечик», криптографический алгоритм, индивидуальный ключ, min-энтропия, генератор случайных последовательностей, сеть Фейстеля.*

***Аннотация***

*Цель статьи: разработка метода генерации криптостойких псевдослучайных последовательностей (ПСП), применимых в задачах защиты данных на основе алгоритма блендера.*

*Методы исследования: методика генерации ПСП на основе криптостойких алгоритмов в соответствии с рекомендациями NIST SP 800-90. Методика тестирования: NIST. Сравнение и оценка качества ПСП с помощью min-энтропии, критерия Пирсона и линейной сложности.*

*Полученный результат: предложен метод генерации криптостойких ПСП, применимых при защите информации в киберфизических системах. Метод основан на использовании блендера в качестве средства генерации ПСП, а также механизма расширения ключей криптоалгоритма блочного шифрования ГОСТ Р 34.12-2015 «Кузнечик». Такой механизм позволяет получать индивидуальные ключи для генерации каждого блока, из которых формируется выходная последовательность, что обеспечивает повышение её криптостойкости. Алгоритм блендера позволяет генерировать блоки произвольной длины. Дополнительная случайность вводится за счет специальной структуры итерационных констант, содержащих секретную ключевую информацию. Оценка качества выходных последовательностей проведена на основе значений min-энтропии, критерия Пирсона и профиля линейной сложности. Исследование статистических свойств последовательностей и их степени случайности выполнялось с помощью пакетов NIST SP 800-22 и NIST 800-90B. Подтверждено высокое качество генерируемых последовательностей.*

*Научная и практическая значимость: разработка и оценка эффективности метода генерации ПСП с помощью блендера, основанного на применении ключей, индивидуальных для каждого блока выходной последовательности. Использование блендера позволяет получать блоки произвольной длины. Высокая скорость работы блендера и простота его алгоритма дают возможность применять предложенный метод генерации в приложениях информационной безопасности на различных платформах для киберфизических систем с ограниченными ресурсами. Кроме того, предложенная схема генерации позволяет легко распараллеливать вычислительные процессы в целях повышения скорости генерации.*

**DOI: 10.24412/1994-1404-2025-1-141-152**

## Введение

В области обеспечения информационной безопасности киберфизических систем (КФС), использование которых неуклонно растет в самых разных сферах деятельности, особое место занимают задачи, относящиеся к разнообразным системам, обладающим низкими ресурсами и в силу этого не обеспеченным достаточной защитой. Регулярный обмен информацией, необходимой для их функционирования, и всё более высокий уровень угроз требуют совершенствования методов и средств криптографической защиты передаваемых данных [1—3]. Это относится к оборудованию Интернета вещей [4], беспилотному транспорту [5], носимым медицинским устройствам [6] и т. п.

[1] ***Грозов Владимир Андреевич, п****реподаватель факультета БИТ Университета ИТМО, г. Санкт-Петербург, Российская Федерация. ORCID: 0000-0002-7998-8175.*

*E-mail: vagrozov@itmo.ru*

[2] ***Будько Михаил Юрьевич,*** *кандидат технических наук, доцент факультета БИТ Университета ИТМО, г. Санкт-Петербург, Российская Федерация. ORCID: 0000-0002-1444-277X.*

*E-mail: mbudko@itmo.ru*

[3] ***Гирик Алексей Валерьевич,*** *кандидат технических наук, доцент факультета БИТ Университета ИТМО, г. Санкт-Петербург, Российская Федерация. ORCID: 0000-0002-4021-7605.*

*E-mail: avg@itmo.ru*

Важной частью криптографических методов являются специальные ГПСП: генераторы псевдослучайных последовательностей (ПСП), создающие ПСП, близкие по свойствам к действительно случайным. Существует множество работ, описывающих как конструкцию ГПСП, так и способы улучшения качества получаемых ПСП и точности оценки их свойств. Продолжаются исследования, связанные с разнообразными подходами к генерации ПСП. При этом происходят как поиск новых алгоритмов, так и модификация существующих с целью повышения качества и криптостойкости создаваемых ПСП.

Широко используемые и простые генераторы ПСП, основанные на сдвиговых регистрах с линейной обратной связью (РСЛОС), обладают высокой производительностью. Однако такие генераторы из-за своей линейности неустойчивы к криптографическим атакам и не подходят для приложений криптографической защиты. Тем не менее предлагаются меры, направленные на повышение криптостойкости таких генераторов за счет различных вариантов внесения нелинейности в их алгоритмы. Например, в [7] разрабатывается метод получения ПСП на основе нечеткой логики. В [8] рассматриваются линеаризованные варианты генерации криптографических ПСП на основе клеточных автоматов. В работе предлагается алгоритм использования полученных ПСП в системах аутентификации и проверки целостности данных. Простота процедуры линеаризации дает возможность применения указанного способа генерации в системах, работающих в режиме реального времени. В [9] генерация ПСП выполняется на базе рекурсивного алгоритма вычисления кубических радикалов, что обеспечивает неограниченную длину последовательностей и отсутствие периодичности их элементов.

Повышение случайности некоторых выходных последовательностей КСГПСП может быть достигнуто за счет использования физических источников энтропии. В статье [10] представлен новый метод генерации псевдослучайных чисел, основанный на дискретных одинаково распределенных источниках колебаний. Однако такие разработки сложны в использовании для многих объектов криптографической защиты из-за их ограниченных ресурсов. Более применимыми представляются генераторы, построенные с помощью криптоалгоритмов, использующие в качестве начального ключа последовательности, близкие по своим свойствам к истинно случайным. В связи с этим наиболее активно используются схемы генерации ПСП, основанные на проверенных криптоалгоритмах, поскольку они дают гарантированное преимущество с точки зрения криптографической безопасности. Например, для получения случайных битов желаемого качества из случайных показаний датчиков БПЛА в [11] используется процесс перемешивания, основанный на потоковом шифре RC4. В работе [12] обсуждается метод генерации ПСП с использованием хэш-функции, основанный на алгоритмах блочного шифрования PRESENT-80 и PRESENT-128.

Необходимость обеспечения информационной безопасности КФС с низким уровнем ресурсов для генерации ПСП приводит к использованию облегченных криптографических алгоритмов [13—15]. Существуют различные решения, позволяющие сохранить баланс между снижением стоимости генерации ПСП и степенью их криптостойкости. Например, в [16] предлагается криптографическая генерация ПСП на основе облегченного блочного криптографического алгоритма Speck, модифицированного путем включения новой функции генерации ключей для повышения случайности выходных данных ПСП.

При всем разнообразии инструментов и подходов, одной из важнейших задач при разработке ГПСП, используемых для задач информационной безопасности, является обеспечение их криптостойкости. Многие распространенные способы ее решения, например, основанные на сложности используемых алгоритмов или увеличении количества циклов шифрования, вряд ли применимы для систем с ограниченными ресурсами. Таким образом, поиск новых быстрых и недорогостоящих методов получения криптографически стойких ПСП является актуальной задачей.

В статье рассматривается метод генерации ПСП на основе блендера[4], который удовлетворяет этим требованиям. Его структура позволяет получать последовательности, состоящие из блоков произвольной длины. Целью работы является повышение криптографической стойкости генерируемых последовательностей. Эта цель достигается за счет использования индивидуальных ключей и внесения дополнительной случайности в формирование каждого блока ПСП.

## 1. Материалы и методы

### Подходы к генерации криптографически стойких ПСП

Эффективным способом генерации криптографически стойких ПСП является использование алгоритмов блочного шифрования в режимах обратной связи по выходу (OFB) и счетчика (CTR). В этих режимах блочные шифры работают по принципу поточного шифрования. Криптостойкость выходных последовательностей генераторов, реализованных таким образом, определяется стойкостью используемых алгоритмов. Обобщение результатов многочисленных исследований позволяет выделить следующие распространенные методы повышения криптостойкости, связанные с ключами, используемыми в алгоритмах генерации ПСП.

[4] Dodis Y., Elbaz A., Oliveira R., Raz R. Improved randomness extraction from two independent sources. In: K. Jansen, S. Khanna, J.D.P. Rolim, D. Ron (eds). Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques. RANDOM APPROX. 2004. Lecture Notes in Computer Science. Vol. 3122. Springer, Berlin, Heidelberg. Pp. 334–344. DOI: 10.1007/978-3-540-27821-4_30 .

- Частая смена ключевых последовательностей. Подобный подход реализован в технологиях распределения ключей («блуждающие ключи»).
- Внесение дополнительной случайности в ключевые последовательности. Это эффективно при наличии доступных и недорогих высококачественных источников случайных данных.
- Изменение размера ключа. Традиционный подход предполагает увеличение размера ключа.

### Блендер как инструмент получения качественных ПСП

Важным вопросом при изучении способов генерации ПСП, близких по свойствам к истинно случайным последовательностям, является возможность их получения из слабых источников случайности. В работе авторов Santha и Vazirani[5] доказано, что из нескольких потоков битов со слабой степенью случайности возможно получение потока битов бóльшей случайности. Дальнейшие исследования в этом направлении привели к разработке серии экстракторов случайности для слабых источников. Одним из таких экстракторов является указанный выше блендер. Простой алгоритм блендера обеспечивает высокую скорость его работы и позволяет получать последовательности высокого качества при невысоких требованиях к входным потокам. Корректная работа блендера достигается при определенном уровне суммарной min-энтропии входных последовательностей.

В работах [17, 18] рассматривалась возможность построения ГПСП с использованием блендера в качестве основного алгоритма на всех этапах работы генератора, а также оценивался уровень криптостойкости его выходных последовательностей.

Блендер преобразует две входные битовые последовательности $x = \{x_0, \ldots, x_{l-1}\}$, $y = \{y_0, \ldots, y_{l-1}\}$ длины $l$ в одну битовую последовательность $z = \{z_0, \ldots, z_{l-1}\}$ той же длины. Аналитически результат работы блендера можно записать, используя набор из $l$ бинарных матриц полного ранга A$\ell$:

$$\begin{aligned} &\mathrm{BLE}_A : \{0,1\}^l \times \{0,1\}^l \to \{0,1\}^l : (x,y) \to \\ &\to \{0,1\}^l : (x,y) \to \left( \left( A_1 x \right) \cdot y, \ldots, \left( A_l\ x \right) \cdot y \right) \end{aligned} \qquad (1)$$

Здесь $A_i x$ — матричное произведение $A_\ell$ на вектор $x$, символ « · » обозначает скалярное произведение $(i = 0, \ldots, l\text{-}1)$. Алгебраические операции над битовыми последовательностями рассматриваются в поле Галуа GF(2) и трактуются следующим образом: умножение эквивалентно логическому И, а сложение — логическому XOR.

Существуют различные варианты построения указанных матриц; например, предлагается способ, при котором начальная матрица набора является единичной, а каждая последующая получается в результате выполнения циклического сдвига вправо столбцов предыдущей матрицы и операции XOR над первым столбцом результата сдвига и соответствующим базисным вектором, полученным в поле Галуа[6]. При этом доказывается, что блендер описанной конструкции обеспечивает экстракцию бóльшего количества случайных битов, чем другие ранее разработанные экстракторы для двух слабых источников.

Важным преимуществом блендера является также возможность варьированием длин входных последовательностей получать на выходе любое требуемое количество битов.

### Механизм расширения ключей шифра «Кузнечик»

Для последующего использования в схеме генерации ПСП выбран механизм расширения ключей алгоритма блочного шифрования «Кузнечик» (ГОСТ Р 34.12-2015). Этот криптоалгоритм сочетает высокую криптостойкость и производительность с простотой реализации. Расширение ключей производится на основе сети Фейстеля, на каждой итерации которой выполняются линейное и нелинейное преобразования (соответственно L и S). Сеть Фейстеля относится к распространенным и эффективным элементам криптографических алгоритмов. Обычно при шифровании выполняется несколько итераций сети Фейстеля с использованием одного набора входных данных, что приводит к перемешиванию и рассеиванию битов выходных ПСП, и, следовательно, повышает криптостойкость алгоритма шифрования. Сеть Фейстеля является удобным инструментом получения требуемого количества индивидуальных ключей. С учетом возможностей блендера для получения его входных последовательностей можно ограничиться одной итерацией. Еще одной привлекательной особенностью «Кузнечика» является наличие в нем итерационных констант $C_i$, которые, будучи преобразованы определенным образом, позволяют вносить дополнительную неопределенность во входные последовательности блендера. Благодаря включению в состав $C_i$ значения счетчика генерация ПСП будет выполняться в режиме CTR. Таким образом, дополнение блендера модифицированным механизмом расширения ключей «Кузнечика» будет способствовать повышению криптостойкости результата генерации.

### Методика оценивания качества ПСП

Исследование качества выходных последовательностей блендера проводилось с помощью оценки их линейной сложности, близости характера распределения к равномерному, статистических свойств и уровня

[5] Santha M., Vazirani U.V. Generating quasi-random sequences from slightly-random sources. J. of Computer and System Sciences. 1986. Vol. 33 (1). Pp. 75–87. DOI: 10.1109/SFCS.1984.715945 .

[6] Johnston D. Random Number Generators—Principles and Practices. A Guide for Engineers and Programmers. DeG Press, 2018. 436 p.

min-энтропии. Min-энтропия определяется для независимой дискретной случайной величины $X$, принимающей значения $X = \{x_1, \mathrm{K}\ x_k\}$ с вероятностями $p_i$, как

$$H = \min_{1 \le i \le k} \left(-\log_2 p_i\right) = -\log_2 \left(\max_{1 \le i \le k} p_i\right) \quad (1)$$

и используется в качестве основной меры непредсказуемости случайной величины.

Числовые характеристики выходных ПСП были рассчитаны с использованием пакетов тестов NIST 800-22[7] и NIST 800-90B[8] (оценка статистических свойств и минимальной энтропии). Близость распределения выходных данных к равномерному определялась с помощью критерия Пирсона. Был построен также профиль линейной сложности, который является одной из мер криптографического качества ПСП [19].

## 2. Результаты

### Аналитическое описание блендера

Блендер может быть описан различными способами, что позволяет выбирать наиболее удобные для решения поставленных задач. Исследование математических свойств блендера выполнялось с помощью теоретического подхода к его построению[9]. Для его аппаратной реализации наиболее эффективны логические схемы, а для целей программирования и исследования характеристик криптостойкости нелинейных преобразований блендера наиболее удобным является его представление в виде набора булевых функций[10].

Рассмотрим подробнее алгоритм построения матриц блендера и получим их явные выражения. Далее будем использовать следующие обозначения: $A_k$ — матрицы размерности $l \times l$, определяющие структуру блендера; $B_k$ — базисные векторы-столбцы $l \times 1$; $E$, $O$ — единичная и нулевая матрицы размерности $l \times l$; $k = 0, \ldots, l-1$.

В качестве начальной матрицы $A_0$ выбирается некоторая сильно разреженная матрица полного ранга размерностью $l \times l$. Базисные векторы $B_k$ формируются как последовательности значений $1, 2^1, 2^2, 2^3, \ldots, 2^{l-1}$, вычисленных в поле Галуа с помощью примитивного многочлена степени $l$. В силу существующего между полем Галуа GF($2^l$) и поля $\{0,1\}^l$ изоморфизма эти векторы могут быть записаны в виде битовых последовательностей. Из их первых $l$ элементов формируются базисные векторы $B_k$.

Процесс построения матриц, определяющих структуру блендера $A_k$, можно описать следующим образом.

1. Выбор начальных значений матриц и векторов. В качестве начальной матрицы $A_1$ размерностью $l \times l$ может быть выбрана единичная матрица $A_0^{ij} = E^{ij}$.

2. Формирование базисных векторов $B_k$ как последовательности первых $l$ значений $1, 2^1, 2^2, 2^3, \ldots, 2^{l-1}$, элементов поля Галуа, вычисленных с помощью некоторогопримитивногомногочлена.Этивекторымогут быть записаны в виде битовых последовательностей. Например, для случая размерности блендера $l = 4$ десятичной последовательности $\{1, 2, 4, 8, 3, 6, 12, 11, 5, 10, 7, 14, 15, 13, 9\}$ соответствует двоичная последовательность $\{0001, 0010, 0100, 1000, 0011, 0110, 1100, 1011, 0101, 1010, 0111, 1110, 1111, 1101, 1001\}$. Из ее первых $l$ членов и формируются базисные векторы $B_k$. В этом случае неприводимый многочлен имеет вид $x^4+x+1$.

3. Каждая следующая матрица $A_k$ вычисляется путем циклического сдвига предыдущей матрицы вправо на один столбец (матрица $\tilde{A}_k$) и последующего выполнения операции XOR (⊕) над 1-м столбцом сдвинутой матрицы и соответствующим базисным вектором $B_k$:

$$\begin{aligned} &\tilde{A}_k = A_{k-1}^{l-(l-j+1) \bmod l}, \\ &A_k = (\tilde{A}_k \oplus B_k, \tilde{A}_k, \ldots, \tilde{A}_k), \\ &j = 1, \ldots, l;\ k = 1, \ldots, l-1. \end{aligned} \quad (2)$$

Эквивалентное описание работы блендера с помощью булевых функций выглядит следующим образом:

$$\begin{aligned} f_0 &= x_{l-1}y_{l-1} \oplus x_{l-2}y_{l-2} \oplus \ldots \oplus x_2y_1 \oplus x_0y_0, \\ f_1 &= x_{l-2}y_{l-1} \oplus \ldots \oplus x_1y_2 \oplus x_0x_{l-1}y_1 \oplus x_{l-1}y_0, \\ &\mathrm{K} \\ f_{l-1} &= x_0x_{l-1}y_{l-1} \oplus x_{l-1}x_{l-2}y_{l-2} \oplus \ldots \oplus x_2x_1y_1 \oplus x_1y_0. \end{aligned} \quad (3)$$

Алгебраические операции над битовыми последовательностями рассматриваются в поле Галуа GF(2) и трактуются следующим образом: умножение эквивалентно логическому И, а сложение — логическому XOR (⊕). Знак логического И ( ∧ ) опускается.

На основе явного выражения для матриц блендера и его представления в виде набора булевых функций выполнена реализация алгоритма.

### Генерация ПСП с помощью блендера

Генерация блоков выходных ПСП осуществляется с помощью блендера в сочетании с элементами механизма расширения ключей шифра ГОСТ Р 34.12-2015 «Кузнечик». Возможность получения ПСП, необходимых для корректной работы блендера даже при использовании минимального числа итераций сети Фейстеля, была подтверждена расчетами. Используемые в исходном алгоритме шифра ГОСТ Р 34.12-2015 итерационные константы определяются простым счетчиком, однако они допускают модификацию, направленную на повышение

[7] Rukhin A., Soto J., Nechvatal J., *et al*. A statistical test suite for random and pseudorandom number generators for cryptographic applications. National Institute of Standards and Technology Special Publication 800–22, revision 1a, 2010.

[8] Turan M., Barker E., Kelsey D., *et al*. Recommendation for the Entropy Sources Used for Random Bit Generation (Draft NIST Special Publication 800–90B). National Institute of Standards and Technology, 2018. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf

[9] Dodis Y., *et al*., 2004.

[10] Johnston D., 2018.

криптостойкости. С помощью такого счетчика генерацию ПСП можно выполнять в режиме CTR.

Повышение криптостойкости в предлагаемом методе генерации базируется на применении блендера и использовании индивидуального ключа для получения очередного блока ПСП. Кроме того, для внесения в алгоритм генерации дополнительной неопределенности служат итерационные битовые константы $C_i$ длины $l$, сформированные специальным образом.

Вначале рассмотрим задачу формирования входных последовательностей для блендера, которые в дальнейшем будут играть роль ключа и вектора инициализации. Их получение состоит в создании выходного потока битов длиною $m \times l$ (m — количество блоков) из короткого ключа длиною $2l$. Для решения этой задачи построен алгоритм на базе модернизированного механизма расширения ключей шифра ГОСТ Р 34.12-2015 «Кузнечик», использующего линейное ($L$) и нелинейное ($S$) преобразования.

Поскольку блендер предназначен для работы со слабыми источниками, допустимо некоторое снижение требований к его входным последовательностям, поэтому для сокращения времени работы алгоритма количество итераций при генерации блока выходного потока уменьшено с восьми (оригинальный алгоритм) до одной.

Предлагаемый метод генерации основан на применении блендера в сочетании с модифицированной сетью Фейстеля. Схема процесса генерации ПСП представлена на рис. 1, *а*. Модификация сети Фейстеля происходит следующим образом. На каждой ее итерации формируются новые значения ключа $K$ и вектора инициализации $IV$, которые являются входными последовательностями блендера. При этом каждая итерация сети Фейстеля работает со своим набором входных данных. Таким образом, каждый блок последовательности генерируется с помощью индивидуальных ключа и вектора инициализации. Общее количество итераций сети Фейстеля равно $m$.

Перед началом генерации очередной ПСП задаются уникальные значения мастер-ключа $MK(K_0)$ и сеансового ключа $SK(IV_0)$. Их преобразование в соответствии со схемой g дает первые входные последовательности блендера — $K_1$ и $IV_1$ соответственно (рис. 1, *б*).

Отличительной особенностью предлагаемой схемы является совмещение в пределах одной итерации сети Фейстеля как генерации очередного блока ПСП, так и обновление входов блендера — ключа и вектора инициализации, с помощью которых будет формироваться следующий блок ПСП.

Перед подачей на блендер вектор инициализации и ключ модифицируются следующим образом. Во-первых, над значением ключа и итерационной константы $C_i$ выполняется операция XOR, после чего к ее результату последовательно применяются преобразования $S$ и $L$ алгоритма «Кузнечик». Результатом этих преобразований является новое значение ключа (функция $g$). Во-вторых, вектор инициализации модифицируется с помощью побайтового циклического сдвига влево. Для его программной реализации используется команда ассемблера ROL. Величина сдвига определяется тремя младшими битами, взятыми из каждого байта результата операции XOR над очередной ключевой последовательностью $K_i$ и итерационной константой $C_i$ (функция $f$, рис. 1, *в*). Использование циклического сдвига связано с тем, что он сохраняет баланс значений 0 и 1 во входных последовательностях, необходимый для корректной работы блендера.

Результат работы блендера образует очередной блок выходной ПСП генератора $Z_i$. Перед началом следующей итерации сети Фейстеля вектор инициализации и ключ меняются ролями и преобразовываются аналогичным образом.

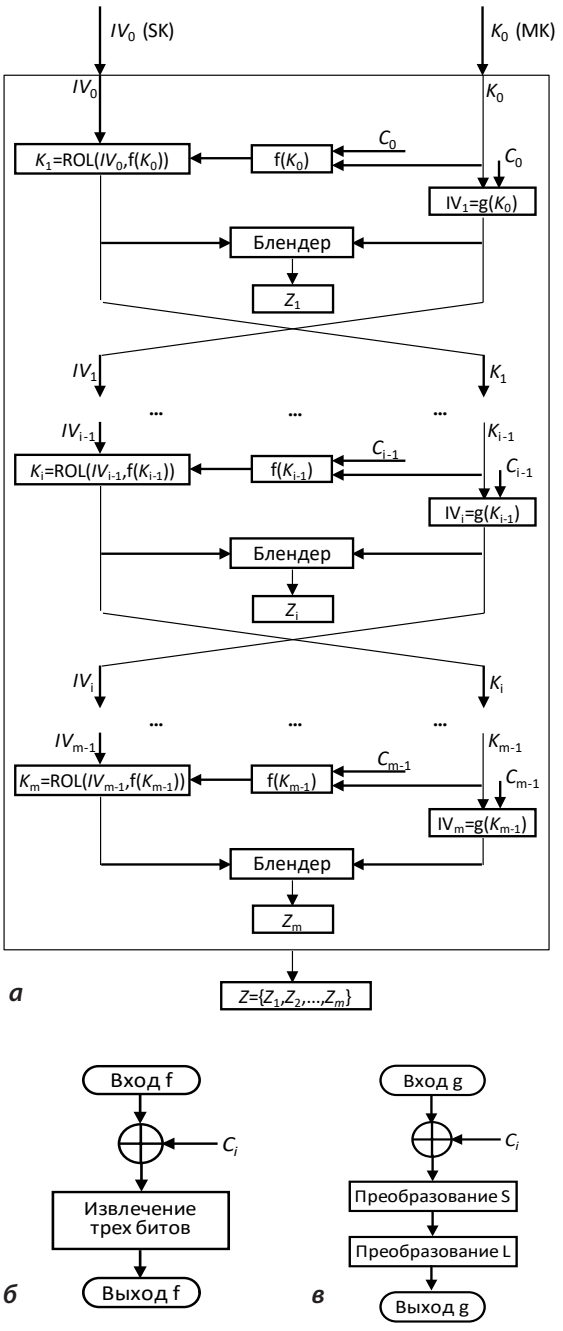



***Рис. 1. Процесс генерации ПСП:***
***а — общая схема, б — функция f, в — функция g***

Процедура формирования итерационных констант $C_i$ состоит в применении линейного преобразования $L$ алгоритма «Кузнечик» к счетчику итераций $c_i$, изменяющемуся с каждой новой итерацией. Начальное заполнение счетчика итераций ($c_0$) выполняется следующим образом:

$$c_0 = (MK \wedge SK) \oplus MK. \quad (4)$$

Далее на каждой итерации значение счетчика $c_0$ сдвигается влево на число битов, необходимое для размещения номера итерации ($i$). Освободившиеся младшие биты заполняются значащими разрядами счетчика. Результатом является значение итерационного счетчика $c_i$. Этот метод формирования счетчика устраняет риск, связанный с наличием систематических входных данных. После применения линейного преобразования $L$ к $c_i$ получаются окончательные значения констант $C_i$, которые используются при формировании входных последовательностей блендера.

Таким образом, каждая итерация сети Фейстеля включает модификацию последовательностей $K$ и $IV$, генерацию очередного блока ПСП с помощью блендера, а также смену ролей ключа и вектора инициализации.

### Результаты численного исследования выходных последовательностей

Традиционным подходом при разработке криптостойких ГПСП является применение надежных криптоалгоритмов. Блендер изначально проектировался как экстрактор случайности, поэтому необходимо было провести исследование его возможностей обеспечивать необходимое качество выходных ПСП. Для этого выполнялось исследование качества выходных ПСП блендера по характеристикам, указанным во втором разделе. При этом использовались входные последовательности, разделенные на шесть уровней в соответствии со значениями min-энтропии (бит/байт) (табл. 1). Последовательности, сгенерированные для изучения возможностей блендера, имели длину 1 Мбит. Тестирование проводилось при уровне значимости $\alpha = 0{,}01$. Размерность блендера $l = 128$.

*Таблица 1*

**Значения min-энтропии входных последовательностей**

| Min-энтропия (бит/байт) | Уровень энтропии входных последовательностей | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| Минимальная | 0.7184 | 1.5392 | 2.2088 | 3.3464 | 4.5224 | 6.7192 |
| Максимальная | 0.7192 | 1.5416 | 2.2136 | 3.3592 | 4.5504 | 7.4304 |
| Средняя | 0.7192 | 1.54 | 2.212 | 3.3552 | 4.5344 | 7.1832 |

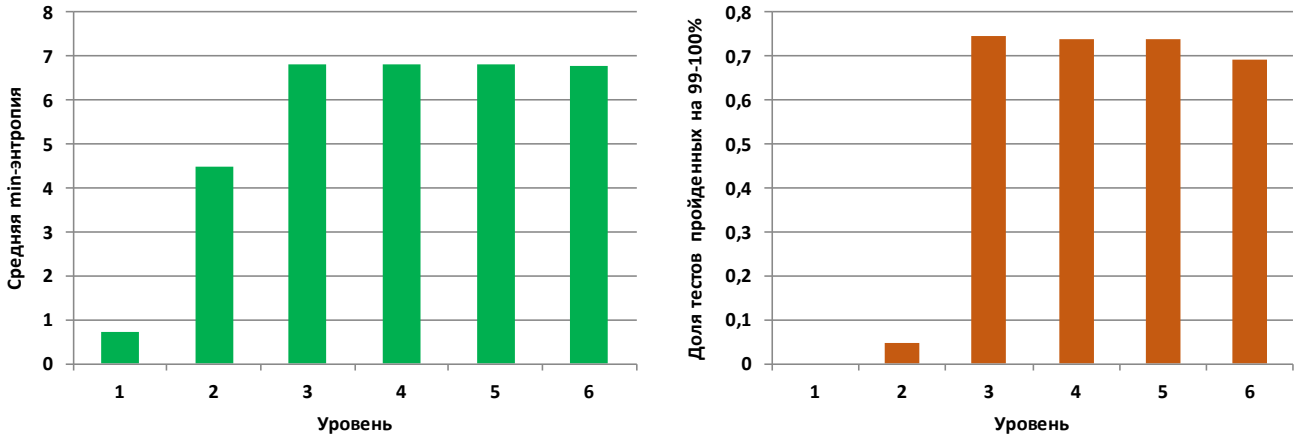
Результаты расчета криптографических характеристик стойкости выходных последовательностей блендера в зависимости от среднего уровня min-энтропии входных последовательностей приведены в табл. 2 и на рис. 2.

*Таблица 2*

**Характеристики выходных последовательностей блендера в качестве экстрактора**

| Min-энтропия (бит/байт) | Уровень энтропии входных последовательностей | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| Минимальная | 0.7152 | 4.4448 | 5.8856 | 5.8856 | 6.4296 | 5.8856 |
| Максимальная | 0.7184 | 4.548 | 7.2976 | 7.2888 | 7.4488 | 7.2432 |
| Средняя | 0.7168 | 4.496 | 6.808 | 6.8032 | 6.8296 | 6.7912 |
| Доля тестов NIST 800-22, пройденных на 99–100% | 0 | 0.048 | 0.745 | 0.739 | 0.739 | 0.691 |
| Критерий Пирсона $\chi^2$ | 1.96·106-1.97·106 | 1.32·105-1.33·105 | 199-318 | 203-301 | 199-318 | 205-305 |

Представленные результаты показывают, что для блендера имеет место существенное влияние исходных данных на результаты работы. В случае блендера неудовлетворительные результаты соответствуют только двум низшим уровням входной min-энтропии. Таким образом, достаточная min-энтропия входных данных должна превышать 2 бит/байт. При этом следует отметить, что уровень min-энтропии, обеспечивающий корректную работу блендера, заведомо превосходит такое значение. Таким образом, блендер обеспечивает необходимый уровень характеристик выходных последовательностей для достаточно широкого диапазона




*а* *б*

***Рис. 2. Средняя min-энтропия (а) и доля пройденных тестов (б) для блендера***

min-энтропии входных данных. В полном соответствии с указанным выше условием корректной работы блендера существует значительное влияние уровня min-энтропии входных последовательностей на качество выходных.

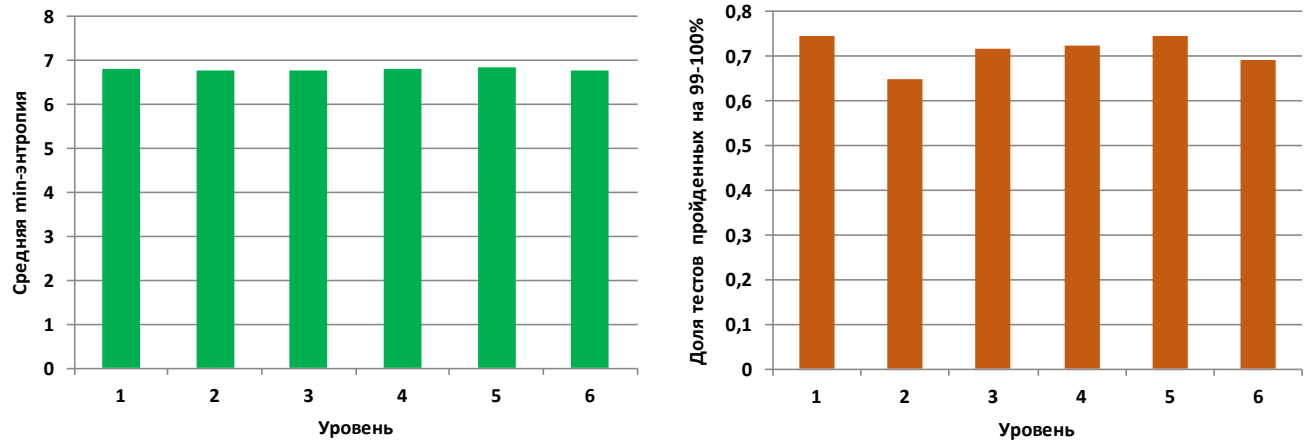
Относительно проверки статистических свойств выходных ПСП блендера следует заметить, что все тесты NIST 800-22 были успешно пройдены, начиная с третьего уровня min-энтропии входных данных. В четвертой строке табл. 2 приведены значения доли тестов NIST 800-22, которые прошли все последовательности.

Представляет интерес сравнение полученных характеристик блендера с аналогичными характеристиками для генератора ПСП (на базе стандартного алгоритма ГОСТ 34-12.2015 «Кузнечик» в режиме OFB). Как видно из табл. 3 и рис. 3, результаты тестирования его выходных последовательностей также говорят об их хорошем качестве и мало зависят от уровня min-энтропии подаваемых на вход данных.

*Таблица 3*

**Характеристики выходных ПСП генератора на основе алгоритма «Кузнечик» в режиме OFB**

| Min-энтропия (бит/байт) | Уровень энтропии входных последовательностей | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| Минимальная | 5.9032 | 5.9032 | 5.9032 | 5.9032 | 5.9032 | 5.9032 |
| Максимальная | 7.3312 | 7.308 | 7.3584 | 7.408 | 7.312 | 7.3048 |
| Средняя | 6.7984 | 6.7832 | 6.7744 | 6.8152 | 6.8608 | 6.7832 |
| Доля пройденных тестов NIST 800-22 (99-100%) | 0.745 | 0.649 | 0.718 | 0.723 | 0.745 | 0.691 |
| Критерий Пирсона $\chi^2$ | 215–332 | 202–342 | 205–301 | 205–304 | 207–302 | 214–314 |




*а* *б*

***Рис. 3. Средняя min-энтропия (а) и доля пройденных тестов (б) для генератора ПСП на базе алгоритма ГОСТ Р 34.12-2015 «Кузнечик»***

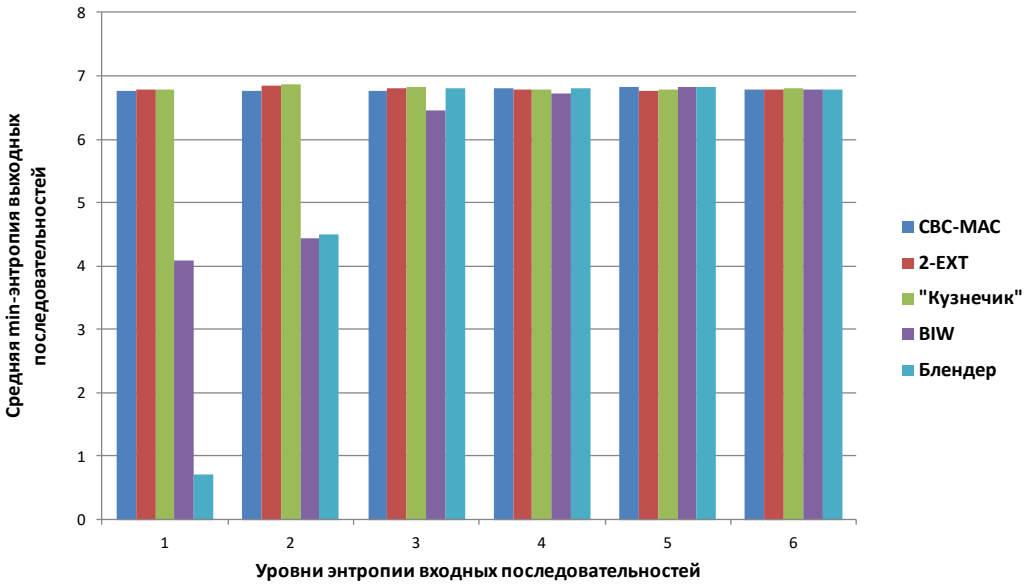



*Рис. 4. Сравнение min-энтропии ПСП при разных вариантах генерации*

*Таблица 4*

**Характеристики выходных последовательностей генератора ПСП на основе блендера**

| Длина ключа, бит | Критерий Пирсона | Min-энтропия | NIST SP800-22 | $R^2$ |
|---|---|---|---|---|
| 40 | 198—328 | 7.138 | 0.686 | 0.99993 |
| 48 | 203—308 | 7.134 | 0.649 | 0.999929 |
| 56 | 172—319 | 7.106 | 0.654 | 0.999927 |
| 64 | 208—303 | 7.125 | 0.665 | 0.999931 |
| 96 | 199—318 | 7.166 | 0.745 | 0.99993 |
| 128 | 203—319 | 7.138 | 0.729 | 0.999928 |
| 256 | 206—319 | 7.146 | 0.707 | 0.999929 |
| 512 | 202—327 | 7.122 | 0.718 | 0.999929 |
| 1024 | 199—307 | 7.136 | 0.718 | 0.99993 |

Таким образом, использование механизма шифра «Кузнечик» обеспечивает нужный уровень min-энтропии в ключах, играющих роль входных последовательностей генератора, созданного на базе блендера.

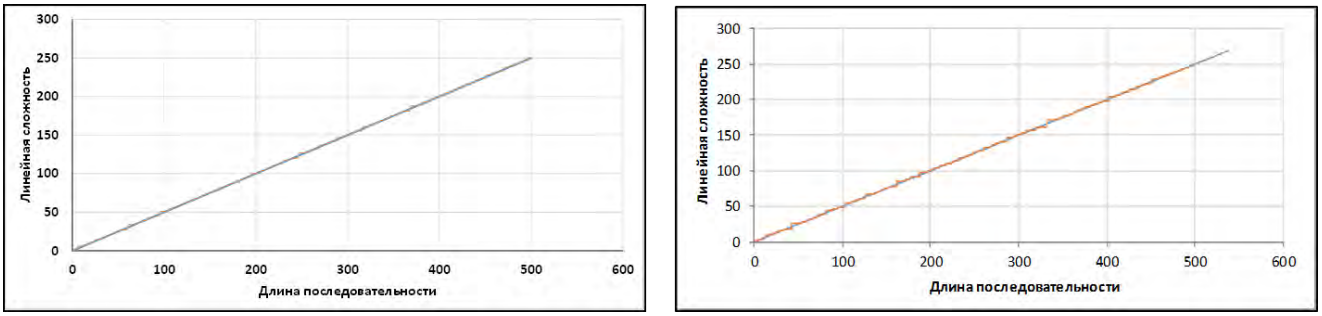
По рассмотренным характеристикам блендер также сравнивался с некоторыми известными экстракторами (CBC-MAC[11], 2-EXT, BIW[12]) и с генератором ПСП, основанном на надежном криптоалгоритме. Первые два средства извлечения используют криптографический алгоритм AES. На рис. 4 представлена диаграмма, позволяющая сравнить среднюю min-энтропию всех рассмотренных экстракторов и генератора псевдослучайных последовательностей на основе алгоритма ГОСТ Р 34.12-2015 «Кузнечик».

Сравнение результатов и по остальным характеристикам показало, что блендер (при корректном его использовании) обеспечивает высокое качество выходных последовательностей. Это подтверждает перспективность использования блендера как ГПСП.

Для изучения качества выходных ПСП, полученных с использованием предложенного метода генерации, были выполнены расчеты их характеристик при различных длинах ключей. Результаты, представленные в табл. 4, соответствуют случаю, когда длины последовательностей, подаваемых в блендер, и длины выход-

[11] E. Barker and D. Kelsey, Recommendation for Random Bit Generator (RBG) Constructions (Draft NIST Special Publication 800–90C). National Institute of Standards and Technology, 2018. URL: https://csrc.nist.gov/csrc/media/publications/sp/800-90c/draft/documents/sp800_90c_second_draft.pdf

[12] Johnston D. Random Number Generators—Principles and Practices. A Guide for Engineers and Programmers. DeG Press, 2018. 436 p.




*а* *б*

***Рис. 5. Профили линейной сложности:***
***а — блендер, б — генератор Блюм-Блюма-Шуба (BBS)***
***(синий цвет — прямая $L_{seq}/2$)***

ных блоков ПСП равны. Для оценки качества выходных данных было сгенерировано 1000 последовательностей по 4 Мбит каждая.

Наряду с показателями min-энтропии, степени прохождения статистических тестов и критерия Пирсона еще одной важной характеристикой криптографической стойкости генератора ПСП является линейная сложность его выходных последовательностей, вычисляемая на основе алгоритма Берлекампа-Мэсси[13]. На рис. 5 показаны диаграммы изменений линейной сложности. Для сравнения представлены аналогичные результаты для генератора Blum-Blum-Shub (BBS), который обладает доказанной высокой криптографической стойкостью[14]. Для всех рассмотренных ПСП линейные профили сложности хорошо аппроксимированы линией $L_{seq}/2$ ($L_{seq}$ — длина последовательности), что указывает на высокую непредсказуемость рассматриваемых ПСП. Численно близость линейного профиля сложности к прямой $L_{seq}/2$ характеризуется значением $R^2$ (approximation confidence value). Его малое отклонение от единицы подтверждает высокую степень случайности исследуемых ПСП.

## 3. Обсуждение

В статье блендер рассматривается как инструмент, способный выполнять не только экстракцию случайности, но и собственно генерацию ПСП. Особенностью блендера является то, что он извлекает максимальную энтропию из относительно слабых источников. С помощью блендера можно также получить выходные ПСП, состоящие из блоков произвольной длины. Поскольку подтверждение криптографической стойкости выходных последовательностей блендера возможно только в результате комплексного исследования, была проведена оценка структуры самого блендера, характеристик ПСП и принципов их создания.

Исследование блендера как совокупности булевых функций, ранее выполненное авторами, показало, что они обладают свойствами, необходимыми для получения криптографически стойких ПСП. Результаты свидетельствуют также о близости характеристик булевых функций блендера ко многим важным характеристикам булевых функций известных криптоалгоритмов (например, AES) [18].

Помимо статистических свойств, исследуемых наиболее часто, рассматривалась min-энтропия как мера непредсказуемости последовательности. Степень близости результирующего распределения к равномерному оценивалась с использованием критерия Пирсона. Кроме того, близость исследуемой ПСП к истинно случайной была оценена с использованием такого значимого показателя, как линейная сложность.

В предложенном методе генерации используется комбинация алгоритма блендера и элементов криптоалгоритма «Кузнечик». Предлагаемый метод сочетает постоянную смену ключа при генерации блоков ПСП и внесение дополнительной случайности во входные данные блендера за счет специальной структуры итерационных констант. Их формирование выполняется с использованием секретного ключа. Таким образом, на каждой итерации (т. е. при формировании следующего блока ПСП) вводится добавочная случайность.

Необходимо особо отметить способность блендера использовать входные последовательности произвольной длины и получать блоки ПСП любой требуемой длины $l$ за одну итерацию. Увеличение размера ключа традиционно рассматривается как положительный фактор с точки зрения криптостойкости. В то же время короткие ключи могут быть эффективны в определенных ситуациях. Например, блендер позволяет из сгенерированных блоков формировать гамму для последующего поточного шифрования. Размер блоков может варьироваться от одного символа до целого сообщения. В первом случае появление любого символа в зашифрованном тексте становится равновероятным, поскольку нарушаются все вероятностно-лингвистические связи алфавита. Во втором случае гамма, генери-

[13] Menezes A., Oorschot P. van, Vanstone S. Handbook of Applied Cryptography. CRC-Press, 1996. 816 p.

[14] Там же.

руемая блендером, превращается в псевдослучайный аналог одноразового блокнота[15].

Кроме того, следует отметить следующие существенные преимущества блендера.

- Произвольный размер выходного блока ПСП.
- Независимость выходных битов от входных значений.
- Влияние входного бита на все выходные биты.

## Выводы

Разработан метод генерации ПСП, основанный на использовании блендера и ключей, индивидуальных для каждого блока выходной последовательности. Генерация ключей осуществляется с использованием модифицированного механизма расширения ключа шифра «Кузнечик», основанного на сети Фейстеля. Чтобы увеличить период последовательности и внести дополнительную случайность, были сформированы итерационные константы специальной структуры. Использование блендера позволяет получать последовательности, состоящие из блоков произвольной длины.

Исследования характеристик полученных ПСП подтвердили их высокое качество и возможность применения предложенного метода генерации в приложениях информационной безопасности для КФС.

Возможность варьирования размерности блендера позволяет реализовать предложенный метод генерации ПСП на различных платформах. Высокая скорость работы блендера и возможность использовать одну итерацию сети Фейстеля для получения блока ПСП обеспечивают высокую производительность генерации. Предлагаемый способ генерации не требует больших затрат памяти, что делает его применимым для устройств с ограниченными ресурсами.

[15] Shannon C. Communication Theory of Secrecy Systems. Bell System Tech. J. 1949. Vol. 28 (4). Pp. 656–715.

**Литература**


1. Котенко И.В., Левшун Д.С., Чечулин А.А. и др. Комплексный подход к обеспечению безопасности киберфизических систем на основе микроконтроллеров // Вопросы кибербезопасности. 2018. № 3 (27). С. 29—38. DOI: 10.21681/2311-3456-2018-3-29-38 .
2. Cyber-Physical Systems: Cyber-Physical Systems: Modelling and Intelligent Control. Studies in Systems, Decision and Control. Vol. 338. A.G. Kravets, A.A. Bolshakov, and M.V. Shcherbakov, Eds. Springer, 2021. DOI: 10.1007/978-3-030-66077-2 .
3. Arshad J., Azad M.A., Amad R., et al. A Review of Performance, Energy and Privacy of Intrusion Detection Systems for IoT. Electronics. 2020. Vol. 9 (629). Pp. 1–24.
4. Perfect Secrecy in IoT: A Hybrid Combinatorial-Boolean Approach. Zolfaghari B., Bibak K., Eds. Springer, 2022. DOI: 10.1007/978-3-031-13191-2 .
5. Syed F., Gupta S.K., et al. A survey on recent optimal techniques for securing unmanned aerial vehicles applications. Trans. emerging telecommunications technologies. 2020. Vol. 32 (1). Pp. 1–34. DOI: 10.1002/ett.4133 .
6. Yaqoob T., Abbas H., Atiquzzaman M. Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices. A Review. IEEE Communications Surveys & Tutorials, 2019. Iss. 4. Pp. 3723–3768. DOI: 10.1109/comst.2019.2914094 .
7. Anikin I.V., Alnajjar K. Secure Data Transmission in Cyber-Physical Systems Based on the New Approach for Stream Cipher's Gamma Generation. In: Cyber-Physical Systems, Springer, 2021. Pp. 333–346.
8. Кулешова Е.А. Методы применения клеточных автоматов в системах защиты информации // Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. 2021. № 2. С. 81—93. DOI: 10.17308/sait.2021.2/3506 .
9. Таныгин М.О., Крыжевич Л.С., Зыков П.С. Разработка генератора псевдослучайных чисел на основе кубических радикалов // Изв. Юго-Зап. гос. университета. 2021. Т. 25 (4). С. 52—69. DOI: 10.21869/2223-1560-2021-25-4-52-69 .
10. Sudeepa K.B., Aithal G. Generation of pseudo random number sequence from discrete oscillating samples of equally spread objects and application for stream cipher system. Concurrency and Computation Practice and Experience. 2019. Vol. 32 (3). Pp. 1–15. DOI: 10.1002/cpe.5181.
11. Cho S.-M., Hong E., Seo S.-H. Random number generator using sensor for drones. Computer Science. IEEE Access. 2020. Vol. 8. Pp. 30343–30354. DOI: 10.1109/ACCESS.2020.2972958 .
12. Susanti B.H., Jimmy J., Ardyani M.W. Evaluation with NIST Statistical Test on Pseudorandom Number Generators based on DMP-80 and DMP-128. In: Proc. of 5th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI). 2022. Pp. 166–171. DOI: 10.1109/ISRITI56927.2022.10053041 .
13. Ullah I., Meratnia N., Havinga P.J.M. Entropy as a service: a lightweight random number generator for decentralized IoT applications. In: Proc. of IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops) (Austin, TX, USA, 2020). 2020. Pp. 1–6. DOI: 10.1109/PerComWorkshops48775.2020.9156205 .
14. Ищукова Е.А., Толоманенко Е.А. Анализ алгоритмов шифрования малоресурсной криптографии в контексте интернета вещей // Современные наукоемкие технологии. 2019. № 3-2. С. 182—186.

15. Khan M.N., Rao A., Camtepe S. Lightweight Cryptographic Protocols for IoT Constrained Devices: A Survey. IEEE Internet of Things. 2021. Vol. 8 (6). Pp. 4132–4156. DOI: 10.1109/JIOT.2020.3026493 .
16. Lustro R.A., Lustro F. Modified Key Derivation Function for Enhanced Security of Speck in Resource-Constrained Internet of Things. I.J. Computer Network and Information Security. 2021. Vol. 13 (4). Pp. 14–25.
17. Grozov V., Guirik A., Budko M., Budko M. Construction of a Cryptographically Secure Pseudorandom Sequence Generator Based on the Blender Algorithm. In: Proc. of 13th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). Virtual, Online, 2021. Pp. 156–161. DOI: 10.1109/ICUMT54235.2021.9631603 .
18. Grozov V., Guirik A., Budko M., Budko M. Cryptographic Strength Study of the Pseudorandom Sequences Generator Based on the Blender Algorithm. In: Proc. of 14th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Valencia, Spain, 2022. Pp. 191–195. DOI: 10.1109/ICUMT57764.2022.9943350 .
19. Гавришев А.А., Осипов Д.Л. Построение обобщенного критерия оценки качества криптостойких кодовых последовательностей, используемых в защищенных беспроводных системах связи // Научное приборостроение. 2023. Т. 33. № 4. С. 111—118.

***SECTION:***
*INFORMATION AND AUTOMATED SYSTEMS AND NETWORKS*

# GENERATING CRYPTOGRAPHICALLY STRONG PSEUDORANDOM SEQUENCES USING A BLENDER

***Vladimir Grozov,*** *Lecturer at the Faculty of Secure Information Technologies of the ITMO University, St. Petersburg, Russian Federation. ORCID: 0000-0002-7998-8175.*
*E-mail: vagrozov@itmo.ru*

***Mikhail Bud'ko,*** *Ph.D. (Technology), Associate Professor at the Faculty of Secure Information Technologies of the ITMO University, Saint Petersburg, Russian Federation. ORCID: 0000-0002-1444-277X.*
*E-mail: mbudko@itmo.ru*

***Alexei Girik,*** *Ph.D. (Technology), Associate Professor at the Faculty of Secure Information Technologies of the ITMO University, Saint Petersburg, Russian Federation. ORCID: 0000-0002-4021-7605.*
*E-mail: avg@itmo.ru*

***Keywords:*** *data protection, GOST R 34.12-2015 Kuznyechik, cryptographic algorithm, individual key, min-entropy, random sequence generator, Feistel network.*

***Abstract***

*Purpose of the paper: development of a method for generating cryptographically strong pseudorandom sequences (PRS) applicable in data protection tasks.*

*Methods used in the study: a technique for generating PRSs based on cryptographic algorithms in accordance with the recommendations of NIST SP 800-90. The NIST testing methodology. Comparison and evaluation of PRS quality using min-entropy, Pearson's criterion and linear complexity.*

*Study findings: a method for generating cryptographically strong PRSs applicable to the protection of information in cyber-physical systems is proposed. The method is based on using a blender as a means of generating PRSs, as well as a mechanism for expanding the keys of block cipher GOST R 34.12-2015 Kuznyechik. This mechanism allows to obtain individual keys for generating each block, from which the output sequence is formed, which ensures an increase in its cryptographic strength. The blender algorithm allows generating blocks of arbitrary length. Additional randomness is introduced due to the special structure of iterative constants containing secret key information. The quality of the output sequences was evaluated by means of the values of min-entropy, the Pearson criterion and the linear complexity profile. The statistical properties of sequences and their degree of randomness were assessed using the NIST SP 800-22 and NIST 800-90B test suits. The high quality of the generated sequences has been confirmed.*

*Research and practical significance: development and evaluation of the efficiency of a method for generating PRSs using a blender, based on the use of keys individual for each block of output sequence. Using a blender allows to generate blocks of arbitrary length. The high speed of the blender and the simplicity of its algorithm make it possible to apply the proposed generation method in information security applications on various platforms for cyber-physical systems with limited resources. In addition, the proposed generation scheme makes it easy to parallelize processes.*

**References**


1. Kotenko I.V., Levshun D.S., Chechulin A.A. i dr. Kompleksnyi podkhod k obespecheniiu bezopasnosti kiberfizicheskikh sistem na osnove mikrokontrollerov. Voprosy kiberbezopasnosti. 2018. No. 3 (27). Pp. 29–38. DOI: 10.21681/2311-3456-2018-3-29-38 .
2. Cyber-Physical Systems: Cyber-Physical Systems: Modelling and Intelligent Control. Studies in Systems, Decision and Control. Vol. 338. A.G. Kravets, A.A. Bolshakov, and M.V. Shcherbakov, Eds. Springer, 2021. DOI: 10.1007/978-3-030-66077-2 .
3. Arshad J., Azad M.A., Amad R., et al. A Review of Performance, Energy and Privacy of Intrusion Detection Systems for IoT. Electronics. 2020. Vol. 9 (629). Pp. 1–24.
4. Perfect Secrecy in IoT: A Hybrid Combinatorial-Boolean Approach. Zolfaghari B., Bibak K., Eds. Springer, 2022. DOI: 10.1007/978-3-031-13191-2 .
5. Syed F., Gupta S.K., et al. A survey on recent optimal techniques for securing unmanned aerial vehicles applications. Trans. emerging telecommunications technologies. 2020. Vol. 32 (1). Pp. 1–34. DOI: 10.1002/ett.4133 .
6. Yaqoob T., Abbas H., Atiquzzaman M. Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices. A Review. IEEE Communications Surveys & Tutorials, 2019. Iss. 4. Pp. 3723–3768. DOI: 10.1109/comst.2019.2914094 .
7. Anikin I.V., Alnajjar K. Secure Data Transmission in Cyber-Physical Systems Based on the New Approach for Stream Cipher's Gamma Generation. In: Cyber-Physical Systems, Springer, 2021. Pp. 333–346.
8. Kuleshova E.A. Metody primeneniia kletochnykh avtomatov v sistemakh zashchity informatsii. Vestnik Voronezhskogo gosudarstvennogo universiteta. Seriia: Sistemnyi analiz i informatsionnye tekhnologii. 2021. No. 2. Pp. 81–93. DOI: 10.17308/sait.2021.2/3506 .
9. Tanygin M.O., Kryzhevich L.S., Zykov P.S. Razrabotka generatora psevdosluchainykh chisel na osnove kubicheskikh radikalov. Izv. Iugo-Zap. gos. universiteta. 2021. T. 25 (4). Pp. 52–69. DOI: 10.21869/2223-1560-2021-25-4-52-69 .
10. Sudeepa K.B., Aithal G. Generation of pseudo random number sequence from discrete oscillating samples of equally spread objects and application for stream cipher system. Concurrency and Computation Practice and Experience. 2019. Vol. 32 (3). Pp. 1–15. DOI: 10.1002/cpe.5181.
11. Cho S.-M., Hong E., Seo S.-H. Random number generator using sensor for drones. Computer Science. IEEE Access. 2020. Vol. 8. Pp. 30343–30354. DOI: 10.1109/ACCESS.2020.2972958 .
12. Susanti B.H., Jimmy J., Ardyani M.W. Evaluation with NIST Statistical Test on Pseudorandom Number Generators based on DMP-80 and DMP-128. In: Proc. of 5th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI). 2022. Pp. 166–171. DOI: 10.1109/ISRITI56927.2022.10053041 .
13. Ullah I., Meratnia N., Havinga P.J.M. Entropy as a service: a lightweight random number generator for decentralized IoT applications. In: Proc. of IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops) (Austin, TX, USA, 2020). 2020. Pp. 1–6. DOI: 10.1109/PerComWorkshops48775.2020.9156205 .
14. Ishchukova E.A., Tolomanenko E.A. Analiz algoritmov shifrovaniia maloresursnoi kriptografii v kontekste interneta veshchei. Sovremennye naukoemkie tekhnologii. 2019. No. 3-2. Pp. 182–186.
15. Khan M.N., Rao A., Camtepe S. Lightweight Cryptographic Protocols for IoT Constrained Devices: A Survey. IEEE Internet of Things. 2021. Vol. 8 (6). Pp. 4132–4156. DOI: 10.1109/JIOT.2020.3026493 .
16. Lustro R.A., Lustro F. Modified Key Derivation Function for Enhanced Security of Speck in Resource-Constrained Internet of Things. I.J. Computer Network and Information Security. 2021. Vol. 13 (4). Pp. 14–25.
17. Grozov V., Guirik A., Budko M., Budko M. Construction of a Cryptographically Secure Pseudorandom Sequence Generator Based on the Blender Algorithm. In: Proc. of 13th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). Virtual, Online, 2021. Pp. 156–161. DOI: 10.1109/ICUMT54235.2021.9631603 .
18. Grozov V., Guirik A., Budko M., Budko M. Cryptographic Strength Study of the Pseudorandom Sequences Generator Based on the Blender Algorithm. In: Proc. of 14th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Valencia, Spain, 2022. Pp. 191–195. DOI: 10.1109/ICUMT57764.2022.9943350 .
19. Gavrishev A.A., Osipov D.L. Postroenie obobshchennogo kriteriia otsenki kachestva kriptostoikikh kodovykh posledovatel'nostei, ispol'zuemykh v zashchishchennykh besprovodnykh sistemakh sviazi. Nauchnoe priborostroenie. 2023. T. 33. No. 4. Pp. 111–118.